ISSN 2225-5435

# Вестник УрФО.

## БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 3(53) / 2024



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

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Свидетельство ПИ № ФС77-65765 от 20.05.2016

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

16+

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

# Journal of the Ural Federal District.

ISSN 2225-5435

**INFORMATION SECURITY**

№ 3(53) / 2024





**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. ФС77-65765 dd. 05/20/2016

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

16+

Electronic version of the magazine in the Internet:
**www.info-secur.ru,**
**e-mail: urvest@mail.ru**

## РАДИОТЕХНИКА, В ТОМ ЧИСЛЕ СИСТЕМЫ И УСТРОЙСТВА ТЕЛЕВИДЕНИЯ



## СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ОБРАБОТКА ИНФОРМАЦИИ



## МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

# IN THIS ISSUE

## RADIO ENGINEERING, INCLUDING TELEVISION SYSTEMS AND DEVICES



## SYSTEM ANALYSIS, MANAGEMENT AND INFORMATION PROCESSING



## METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

УДК 621.396.67.012.12 Вестник УрФО № 3(53) / 2024, с. 5–13

**Баимов Р. И., Соколов А. Н.**

10.14529/secur240301

# *ПРИМЕНЕНИЕ АДАПТИВНОЙ ФАЗИРОВАННОЙ АНТЕННОЙ РЕШЕТКИ ДЛЯ ЗАЩИТЫ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ ОТКРЫТОГО КАНАЛА СВЯЗИ*

*В статье рассмотрены вопросы применения адаптивных фазированных антенных решеток (АФАР) для повышения помехоустойчивости беспроводных сетей передачи и защиты данных по открытому каналу связи. Естественные помехи и постановщики помех представляют угрозу целостности данных, передаваемых по открытому каналу связи. Предложенная антенная система с адаптивной фазированной решеткой использует интеллектуальные методы формирования диаграммы направленности (ДН) антенны, имеющей узкий луч в направлении информационного источника сигнала, глубокие нули ДН в направлении постановщиков помех, а также низкий фон боковых лепестков ДН, снижающих воздействие помех с произвольных направлений. Низкий фон боковых лепестков ДН задаётся подобранными по критериям оптимальности весовыми коэффициентами распределения на элементах АФАР.*

***Ключевые слова:*** *адаптивная фазированная антенная решетка, амплитудное весовое распределение, вектор весовых коэффициентов, разностная диаграмма направленности, суммарная диаграмма направленности, открытый канал связи, помехоустойчивость.*

# THE USE OF AN ADAPTIVE PHASED ARRAY ANTENNA FOR DATA PROTECTION WHEN USING AN OPEN COMMUNICATION CHANNEL

*The article discusses the use of adaptive phased array antennas (AFAR) to increase the noise immunity of wireless transmission networks and data protection over an open communication channel. Natural interference and jammers pose a threat to the integrity of data transmitted over an open communication channel. The proposed antenna system with an adaptive phased array uses intelligent methods for generating a directional pattern (DN) of an antenna having a narrow beam in the direction of the information signal source, deep zeros of the DN in the direction of the jammers, as well as a low background of the side lobes of the DN, reducing the impact of interference from arbitrary directions. The low background of the side lobes of the bottom is set by the weight distribution coefficients selected according to the optimality criteria on the AFAR elements.*

***Keywords:*** *adaptive phased array antenna, amplitude weight distribution, vector of weight coefficients, differential radiation pattern, total radiation pattern, open communication channel, noise immunity.*

**Введение**

В условиях быстрого роста сетей беспроводной связи и развития технологии IoT обеспечение безопасности передаваемых данных стало критически важной задачей. Данные открытого канала связи подвергаются воздействию помех от различных источников, таких, например, как пользователи соседнего и совмещенного каналов, атмосферные условия и внешние электромагнитные сигналы, внешние постановщики преднамеренных помех и т.д. Эти помехи могут нарушать целостность пакетов, передаваемых данных, ухудшать качество сигнала, затрудняя своевременный прием данных [1,2].

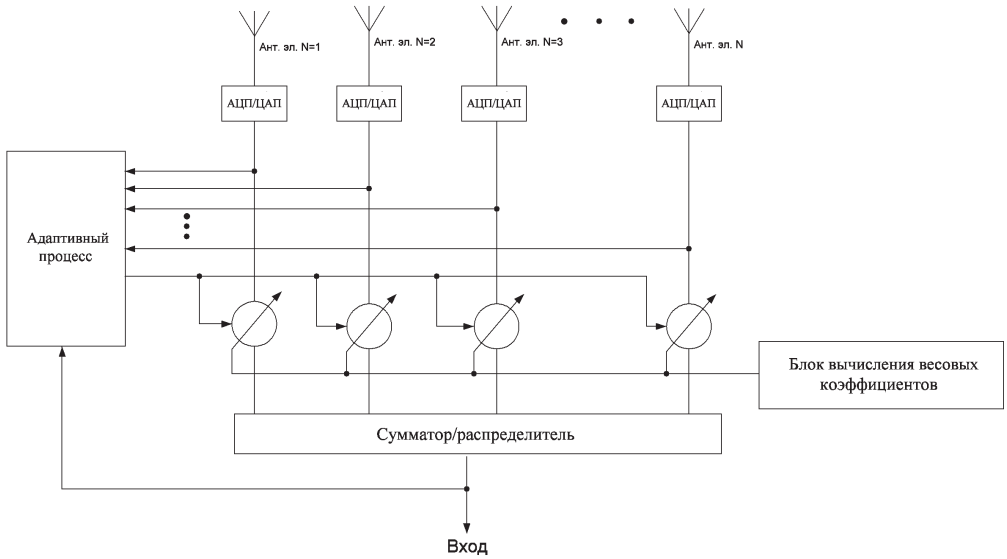


Рис. 1. Функциональная схема АФАР

*Таблица 1*

**ВВК $w_{onm}$ по критериям оптимальности**

| Критерий оптимальности | $w_{onm}$ |
|---|---|
| Оптимальное с общей шириной лепестков | $w_{onm} = \frac{\sin(\pi n / N)}{(\pi n / N)}$ |
| Оптимальное с минимальной боковой лепестковой энергией | $w_{onm} = exp\left\{-\frac{[sin(\pi n / N)]^2}{2\sigma^2}\right\}$ |
| Оптимальное с минимальной суммой квадратов пьедесталов | $w_{onm} = \left\{\begin{matrix} 1, \text{ если } n = 0; \\ \frac{\sin[(\pi n / N)/2]}{[(\pi n / N)/2]}, \text{ если } n > 0 \end{matrix}\right\}$ |
| Оптимальное с минимальной площадью под кривой диаграммы направленности | $w_{onm} = \sqrt{\frac{2}{N}} \cdot \cos\left(\frac{\pi n}{N}\right)$ |
| Оптимальное с минимальным количеством несовпадений фаз | $w_{onm} = \cos\left(\frac{\pi n}{N}\right) + j \cdot \sin\left(\frac{\pi n}{N}\right)$ |
| Оптимальное с наименьшей мощностью на пьедестале | $w_{onm} = \sqrt{\frac{2}{N}} \cdot \cos\left(\frac{\pi n}{N}\right) \cdot \exp\left\{-j \cdot \sin\left(\frac{\pi n}{N}\right)\right\}$ |

где $n$ – порядок весового распределения;

$\sigma$ – стандартное отклонение весовой функции, характеризующее разброс весов элементов антенной решетки;

$N$ – количество элементов линейной фазированной антенной решетки (ЛФАР).

Известны несколько методов защиты от воздействия радиопомех: организационный, энергетический, сигнальный и пространственный [3-5].

Организационный метод основывается на достижение необходимого уровня электромагнитной совместимости между источниками радиоизлучения (ИРИ). Однако этот метод исчерпал своё применение в условиях большой насыщенности ИРИ и ограниченности радиочастотного диапазона.

Энергетический метод борьбы с помехами предусматривает увеличение мощности передатчика до уровня, который гарантированно подавляет возможные помехи. Недостатком метода является повышение затрат на энергоресурсы передатчика ИРИ.

Сигнальный метод борьбы с помехами основывается на фильтрации сигнала путем ограничения полосы пропускания. Это обеспечивается использованием фильтров для удаления нежелательных частот и шума из сигнала. Недостатком метода является способность ослаблять или удалять полезные компоненты сигнала, если они попадают в пределы фильтруемой полосы пропускания. Это может привести к потере информации или ухудшению качества сигнала. К сигнальному методу также можно отнести технологии помехоустойчивого кодирования.

Перспективным методом защиты от помех является пространственная обработка сигналов с помощью адаптивных фазированных антенных решеток (АФАР). АФАР — это антенная система, которая включает в себя массив из нескольких антенн и алгоритма адаптивной обработки сигналов. Метод пространственной обработки автоматически формирует диаграмму направленности АФАР для улучшения приема информационного сигнала на фоне различных помех (рис. 1).

### Формирование оптимального амплитудного распределения на элементах адаптивной фазированной антенной решетки

Формирование распределений амплитуд на основе их критериев оптимальности позволяет снизить уровень боковых лепестков и уменьшить ширину главного лепестка ДН. Это способствует увеличению помехозащищенности открытого канала связи. Изменение вектора весовых коэффициентов (ВВК) от исходного состояния до оптимального ($w_{onm}$) зависит от выбранного критерия оптимальности [6-8].

Выбор критерия оптимальности тесно связан с показателем, количественно измеряющим качество приема полезного сигнала

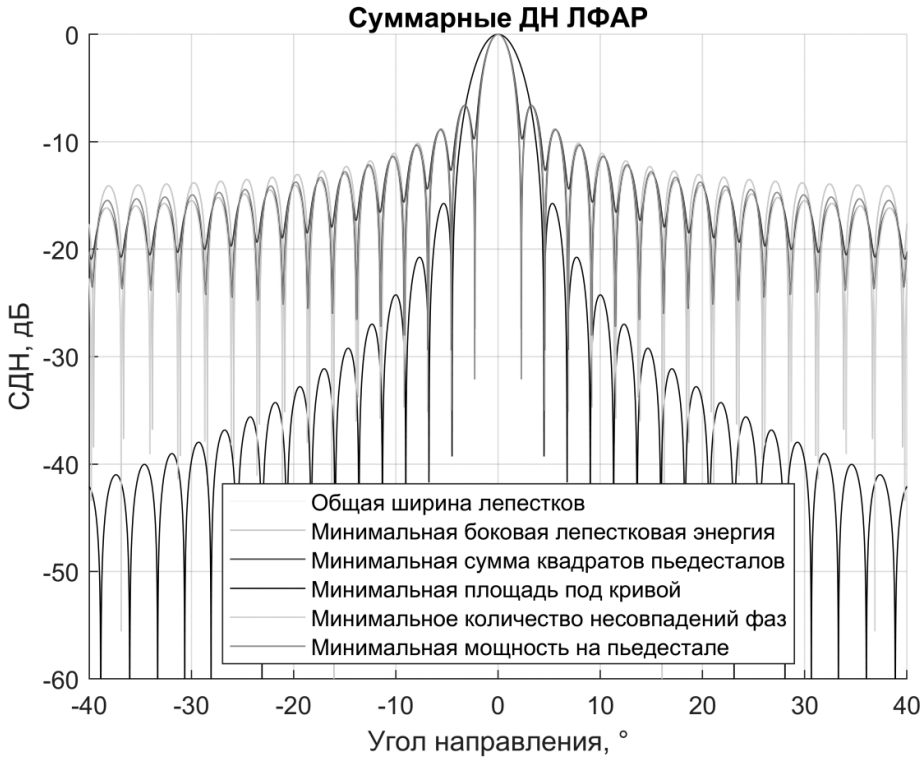


Рис. 2. Результаты расчётов суммарных ДН ЛФАР по критериям оптимальности амплитудных распределений

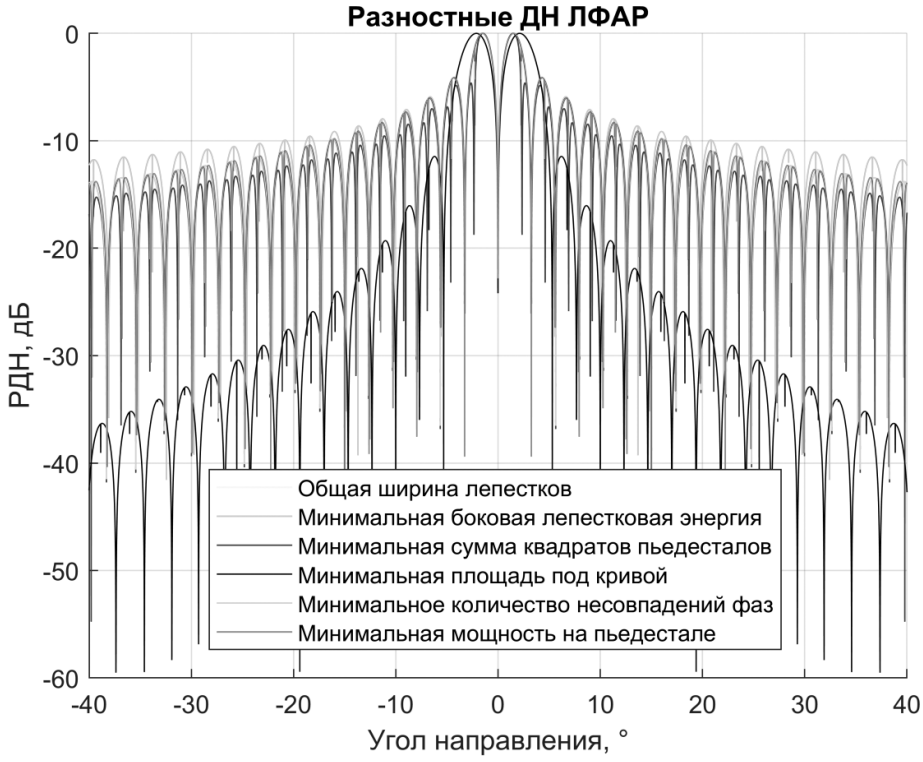


Рис. 3. Результаты расчётов суммарных ДН ЛФАР по критериям оптимальности амплитудных распределений

*Таблица 2*

**Сравнение амплитудных распределений**

| Оптимальные амплитудные распределения | Ширина главного лепестка, град. | Уровень боковых лепестков СДН, дБ | Уровень боковых лепестков РДН, дБ |
|---|---|---|---|
| Оптимальное с общей шириной лепестков | 2,1 | -8,78 | -5,9 |
| Оптимальное с минимальной боковой лепестковой энергией | 2,15 | -8,77 | -5,9 |
| Оптимальное с минимальной суммой квадратов пьедесталов | 2,35 | -8,89 | -7,03 |
| Оптимальное с минимальной площадью под кривой диаграммы направленности | 3,5 | -15,74 | -11,6 |
| Оптимальное с минимальным количеством несовпадений фаз | 2,22 | -8,89 | -6,05 |
| Оптимальное с наименьшей мощностью на пьедестале | 2,18 | -8,86 | -6,01 |

на фоне помех. Целевая функция описывает, как изменяется показатель качества в зависимости от значений весовых амплитудных коэффициентов. Экстремум целевой функции представляет собой критерий оптимальности, которого можно достичь за счет оптимизации функции весовых коэффициентов.

В таблице 1 определены оптимальные ВВК ($w_{опт}$) в зависимости от критерия оптимальности.

На рисунках 2, 3 приведены расчеты суммарных и разностных диаграмм направленности (СДН, РДН) для ранее не представленных оптимальных амплитудных распределений.

Анализ результатов, отображённых на рисунках 2, 3 обобщён в таблице 2.

По данным таблицы 2, наиболее эффективным оптимальным амплитудным распределением является то, что формирует минимальную площадь под кривой диаграммы направленности. Это означает, что такое распределение имеет низкий уровень боковых лепестков СДН и РДН.

Боковые лепестки представляют собой области, где сигнал имеет значительную амплитуду, но не находится в фазе с основным сигналом. Это может привести к помехам и ухудшению качества сигнала. Поэтому оптимальное амплитудное распределение с минимальной площадью под кривой диаграммы направленности обеспечивает низкий уровень боковых лепестков, что позволяет уменьшить влияние помех на канал связи.

Таким образом, данное оптимальное амплитудное распределение является наиболее эффективным для обеспечения помехозащищенности канала связи.

**Формирование глубоких нулей в суммарной диаграмме направленности адаптивной фазированной антенной решеткой в направлении помех**

Формирование глубоких нулей в ДН АФАР заключается в оценке и определении направления на полезный и мешающие ИРИ. Путем адаптации амплитудных распределений на элементах АФАР возможно достижение повышенной помехозащищенности канала связи от преднамеренных помех.

1) Формирование нулей в СДН АФАР в направлении помех определяется выражением (1):

$$СДН = S_п - \frac{S_п S_м S_м^H}{N}, \qquad 1)$$

где $S_п$ – полезный сигнал;

$S_м$ – мешающий сигнал;

$N$ = 16 – количество элементов в ЛФАР (условие моделирования).

Увеличение количества элементов в системе может привести к сужению ширины луча и уменьшению уровней боковых лепестков. При изменении угла падения в большую сторону ДН будет двигаться вправо, в меньшую сторону влево. Но при различных условиях моделирования взаимосвязь между распределениями амплитуд должна оставаться постоянной [9].

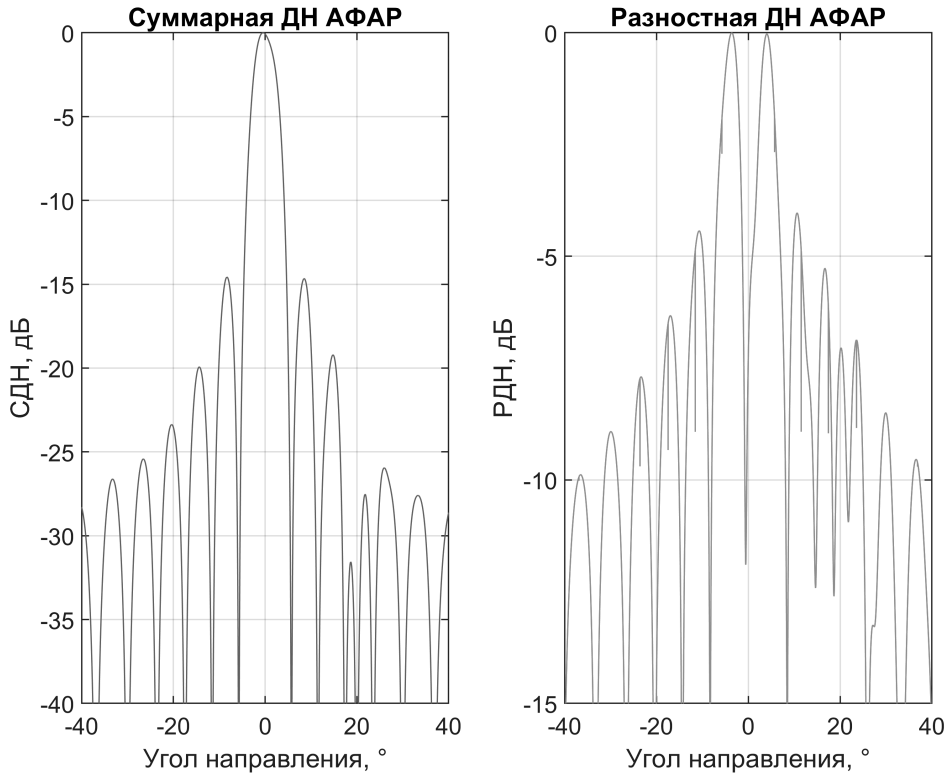


Рис. 4. Результаты расчётов СДН и РДН с нулем в направлении помехи

Определение полезного и мешающего сигнала осуществляется с использованием системы «свой-чужой». Для достижения этой цели в приемном устройстве применяется спектральный анализатор АФАР, который обеспечивает возможность выделения полезных сигналов от мешающих. Такой подход позволяет повысить точность и эффективность обработки сигналов, что критически важно для обеспечения надежности работы системы в условиях наличия преднамеренных помех.

На рис. 4 приведены результаты расчётов СДН, РДН с нулями в направлении помех по критериям оптимальности на элементах ЛФАР.

По результатам моделирования на СДН (рис.4) определены полезный сигнал в направлении $S_n = 0^\circ$ и мешающий сигнал, поставленный преднамеренной помехой в направлении $S_м = 20^\circ$. Метод формирования глубоких нулей эффективно подавил преднамеренную помеху, подав в данном направлении ноль. Это свидетельствует о сохранении целостности передаваемой информации по открытому каналу связи. Изменение мешающего и полезного сигнала не повлияют на результат моделирования.

**Формирование широких провалов в суммарной диаграмме направленности адаптивной фазированной антенной решеткой в направлении помех**

Широкие провалы в СДН в направлении помех формируются в АФАР путем использования алгоритмов адаптивной обработки сигналов. С помощью алгоритмов адаптивной обработки сигналов производится настройка фаз и амплитуд элементов АР в соответствии с направлением подавления помех в заданном широком угловом секторе. Для моделирования выбран сектор в направлении [–80°;30°]. Изменения данного сектора не повлияют на результаты моделирования.

На рис. 5 приведены результаты расчётов СДН и РДН с широкими провалами в направлении помех при амплитудном распределении по критериям оптимальности на элементах АФАР.

На основании результатов моделирования, выполненного с использованием СДН, (см. рис. 5), были определены полезный сигнал в направлении $S_n = 0^\circ$ и мешающие сигналы, создаваемые преднамеренными помехами в угловом секторе $S_м = [-80^\circ; 30^\circ]$. В результате взятия производной от СДН,

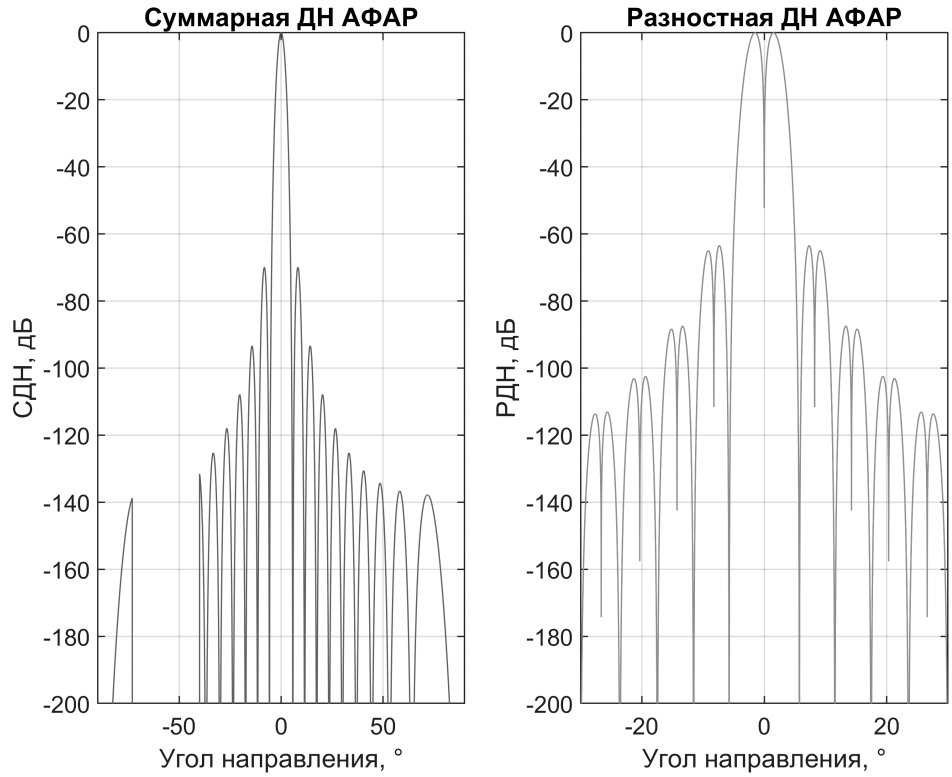


Рис. 5. Результаты расчётов СДН и РДН с широкими провалами в направлении помех

получена РДН, которая демонстрирует более низкий уровень боковых лепестков, по сравнению с методом глубоких нулей (рис. 4). Это свидетельствует о повышенной помехоустойчивости канала связи, при воздействии на него сразу несколько источников помех.

По результатам моделирования, представленного рисунками 4 – 5, наиболее эффективным является комплексный подход в подавлении помех. Это метод формирования широких провалов в направлении помех по критериям оптимальности (рис.5), который обеспечивает минимальную площадь под кривой амплитудного распределения. Метод имеет наименьший уровень боковых лепестков, которые отвечают за помехозащищенность, и может обеспечить подавление нескольких преднамеренных помех в одном направлении (угловом секторе).

**Заключение**

В ходе исследований установлено, что технология АФАР имеет значительный потенциал в обеспечении целостности информации при ее передаче по открытым каналам связи. Путем проведения моделирования и анализа полученных результатов продемонстрирована эффективность метода адаптивного формирования луча с целью уменьшения помех и повышения защиты данных. По результатам анализа данных, приведённых в таблице 2, на рисунках 2 – 5 можно сделать вывод о том, что метод формирования широких провалов в направлении помех по критериям оптимальности (рис. 5), который обеспечивает минимальную площадь под кривой амплитудного распределения и реализует качественную адаптацию АФАР в борьбе с помехами, что позволяет устранить угрозу целостности данных, передаваемых по открытому каналу связи.

## Литература


1. Швырев Б.А. Технический канал утечки информации за счет имитации легального канала стандарта IEEE 802.11 // Швырев Б.А., Цимбал В.Н., Антонов А.С. // Вестник УрФО. Безопасность в информационной сфере. № 3(49) /2023. С. 81–89.

2. Баимов Р.И., Рагозин А.Н. Применение адаптивной фазированной антенной решетки для защиты данных при использовании открытого канала связи / В сборнике: Безопасность информационного пространства. Сборник трудов XXII Всероссийской научно-практической конференции студентов, аспирантов и молодых учёных. Челябинск, 2024. С. 89-95.

3. Ефанов В.И., Тихомиров А.А. Электромагнитная совместимость радиоэлектронных средств и систем. Учебное пособие. – Томск: Томский государственный университет систем управления и радиоэлектроники, 2012. – 228 с.

4. Электромагнитная совместимость и помехозащищённость РЭС: учебное пособие / А.П. Пудовкин, Ю.Н. Панасюк, Т.И. Чернышова. – Тамбов: Изд-во ФГБОУ ВПО «ТГТУ», 2013.

5. Гурина Л.А. Электромагнитные помехи и методы защиты от них: Учебное пособие. / Благовещенск: Амурский гос. ун-т, 2006.

6. Рагозин А.Н., Баимов Р.И. Повышение точности пеленгования источника радиоизлучения за счет выбора оптимального амплитудного весового распределения антенной решетки в составе радиоугломерной посадочной системы / журнал «Приборы» №8, 2024.

7. Баимов Р.И., Рагозин А.Н. Выбор оптимального весового распределения на элементах фазированной антенной решетки для повышения точности пеленгации источника радиоизлучения/ В сборнике: Автоматизированные системы управления и информационные технологии. Материалы всероссийской научно-технической конференции. Пермь, 2023. С. 232-238.

8. Григорьев В.А., Щесняк С.С., Гулюшин В.Л., Распаев Ю.А., Лагутенко О.И., Щесняк А.С. //Адаптивные антенные решетки. Учебное пособие в 2-ух частях. Часть 1. Санкт-Петербург: СПб: Университет ИТМО, 2016. С. 45-46.

9. Баимов Р. И. Выбор весового окна амплитудного распределения на элементах линейной фазированной антенной решетки по критерию ширина луча - уровень боковых лепестков диаграммы направленности / Р. И. Баимов, А. Н. Рагозин // Инфокоммуникационные технологии: актуальные вопросы цифровой экономики: Сборник научных трудов III Международной научно-практической конференции, Екатеринбург, 25–26 января 2023 года / Под редакцией В.П. Шувалова, сост. М.П. Карачарова. – Екатеринбург: Уральский государственный университет путей сообщения, 2023. – С. 72-77.


## References


1. Shvyrev B.A. Tekhnicheskiy kanal utechki informatsii za schet imitatsii legal'nogo kanala standarta IEEE 802.11 // Shvyrev B.A., Tsimbal V.N., Antonov A.S. // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. № 3(49) /2023. S. 81–89.

2. Baimov R.I., Ragozin A.N. Primeneniye adaptivnoy fazirovannoy antennoy reshetki dlya zashchity dannykh pri ispol'zovanii otkrytogo kanala svyazi / V sbornike: Bezopasnost' informatsionnogo prostranstva. Sbornik trudov XXII Vserossiyskoy nauchno-prakticheskoy konferentsii studentov, aspirantov i molodykh uchonykh. Chelyabinsk, 2024. S. 89-95.

3. Yefanov V.I., Tikhomirov A.A. Elektromagnitnaya sovmestimost' radioelektronnykh sredstv i sistem. Uchebnoye posobiye. – Tomsk: Tomskiy gosudarstvennyy universitet sistem upravleniya i radioelektroniki, 2012. – 228 s.

4. Elektromagnitnaya sovmestimost' i pomekhozashchishchonnost' RES: uchebnoye posobiye / A.P. Pudovkin, YU.N. Panasyuk, T.I. Chernyshova. – Tambov: Izd-vo FGBOU VPO «TGTU», 2013.

5. Gurina L.A. Elektromagnitnyye pomekhi i metody zashchity ot nikh: Uchebnoye posobiye. / Blagoveshchensk: Amurskiy gos. un-t, 2006.

6. Ragozin A.N., Baimov R.I. Povysheniye tochnosti pelengovaniya istochnika radioizlucheniya za schet vybora optimal'nogo amplitudnogo vesovogo raspredeleniya antennoy reshetki v sostave radiouglomernoy posadochnoy sistemy / zhurnal «Pribory» №8, 2024.

7. Baimov R.I., Ragozin A.N. Vybor optimal'nogo vesovogo raspredeleniya na elementakh fazirovannoy antennoy reshetki dlya povysheniya tochnosti pelengatsii istochnika radioizlucheniya/ V sbornike: Avtomatizirovannyye sistemy upravleniya i informatsionnyye tekhnologii. Materialy vserossiyskoy nauchno-tekhnicheskoy konferentsii. Perm', 2023. S. 232-238.

8. Grigor'yev V.A., Shchesnyak S.S., Gulyushin V.L., Raspayev YU.A., Lagutenko O.I., Shchesnyak A.S. // Adaptivnyye antennyye reshetki. Uchebnoye posobiye v 2-ukh chastyakh. Chast' 1. Sankt-Peterburg: SPb: Universitet ITMO, 2016. S. 45-46.

9. Baimov R. I. Vybor vesovogo okna amplitudnogo raspredeleniya na elementakh lineynoy fazirovannoy antennoy reshetki po kriteriyu shirina lucha - uroven' bokovykh lepestkov diagrammy napravlennosti / R. I. Baimov, A. N. Ragozin // Infokommunikatsionnyye tekhnologii: aktual'nyye voprosy tsifrovoy ekonomiki: Sbornik nauchnykh trudov III Mezhdunarodnoy nauchno-prakticheskoy konferentsii, Yekaterinburg, 25–26 yanvarya 2023 goda / Pod redaktsiyey V.P. Shuvalova, sost. M.P. Karacharova. – Yekaterinburg: Ural'skiy gosudarstvennyy universitet putey soobshcheniya, 2023. – S. 72-77.

**СОКОЛОВ Александр Николаевич,** кандидат технических наук, доцент, заведующий кафедрой «Защита информации» федерального государственного автономного образовательного учреждения высшего образования «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: sokolovan@susu.ru

**БАИМОВ Роман Ирекович,** студент кафедры радиоэлектроники и систем связи федерального государственного автономного образовательного учреждения высшего образования «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: baimov.roman@internet.ru

**SOKOLOV Alexander Nikolaevich,** Candidate of Technical Sciences, Associate Professor, Head of Information Security Department, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (National Research University)". 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: sokolovan@susu.ru

**BAIMOV Roman Irekovich,** student Department of Radio Electronics and Communication Systems, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (National Research University)". 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: baimov.roman@internet.ru

УДК 004.942:519.23/.25 Вестник УрФО № 3(53) / 2024, с. 14–25

**Коренев Д. А., Захаров А. А., Ханбеков Ш. И.** 10.14529/secur240302

# *ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ СОЗДАНИЯ ДОПОЛНИТЕЛЬНОГО СЕРВИСА К МИС, РАБОТАЮЩЕЙ С УСТРОЙСТВАМИ ИНТЕРНЕТА МЕДИЦИНСКИХ ВЕЩЕЙ*

*В статье предлагается оригинальный подход для работы врачей с медицинской информацией в домашних медицинских стационарах, позволяющий получить общую картину лечебных мероприятий, проводимых с пациентом в медицинских учреждениях города. Для доступа к медицинской информации о пациенте в больницах и поликлиниках города предлагается использовать дополнительную Блокчейн базу (блокчейн из блокчейнов) в качестве распределенного безопасного информационного хранилища актуальных медицинских данных из независимых информационных систем городских поликлиник, стационаров и домашних стационаров. Представлена архитектура хранилища, описаны структуры хранения данных и предложен псевдокод для создания блокчейна с возможностью добавления информации. Описан прототип системы, включающий сервисы для поиска, получения и обработки информации. Приводятся результаты вычислительных экспериментов, позволяющие оценить производительность прототипа системы. Описан API для работы с Блокчейн базой, использующий в том числе голосового помощника с учетом необходимых требований по защите конфиденциальной медицинской информации.*

***Ключевые слова:*** *информационная безопасность, интернет вещей, блокчейн, медицинская информационная система, телемедицина*

# *THE USE OF BLOCKCHAIN TECHNOLOGY TO CREATE AN ADDITIONAL SERVICE TO THE MIS WORKING WITH THE INTERNET OF MEDICAL THINGS DEVICES*

*The article suggests an original approach for doctors to work with medical in-formation in home medical hospitals, which allows to get an overall picture of the therapeutic measures carried out with the patient in medical institutions of the city. To access medical information about a patient in hospitals and polyclinics of the city, it is proposed to use an additional Blockchain database (blockchain from blockchains) as a distributed secure information repository of up-to-date medical data from independent information systems of urban polyclinics, hospitals and home hospitals. The architecture of the storage is presented, data storage structures are described and a pseudocode for creating a blockchain with the ability to add information is proposed. A prototype of the system is described, including services for searching, receiving and processing information. The results of computational experiments are presented to evaluate the performance of the prototype system. The API for working with the Blockchain database is described, including using a voice assistant, taking into account the necessary requirements for the protection of confidential medical information.*

***Keywords:*** *Information security, Internet of Things, Blockchain, Medical In-formation System, Telehealth*

Для понимания значения и чувствительности медицинской информации важно учитывать следующие аспекты:

1. Личная конфиденциальность. Медицинская информация содержит чувствительные данные о здоровье, медицинских диагнозах, лечении и истории болезней пациентов. Эти данные могут быть крайне частными и личными, и их неправомерное раскрытие и тем более изменение могут нанести серьезный вред личной жизни и достоинству пациента, а также физиологическому духовному здоровью. Отметим, что данные о пациенте могут находиться в различных городских медицинских организациях в МИС от различных поставщиков.

2. Доверие пациентов. Защита медицинской информации является ключевым фактором для поддержания доверия пациентов к медицинским учреждениям и профессионалам. Пациенты должны быть уверены, что их данные будут обрабатываться и храниться с соблюдением высоких стандартов конфиденциальности и безопасности.

3. Этические соображения. Медицинские данные содержат информацию, которая может быть использована для дискриминации или нанесения вреда пациентам. Защита этой информации важна для соблюдения этических принципов и защиты прав пациентов.

4. Законодательство и нормативные требования. Существующее законо-дательство, регулирующее обработку, передачу и хранение медицинской информации предусматривает штрафы и наказания за нарушение конфиденциальности данных. Понимание этих нормативных требований важно для соблюдения законодательства и минимизации рисков.

5. Безопасность и защита от угроз. Медицинская информация может быть целью злоумышленников, которые могут использовать эту информацию для вымогательства, мошенничества или других противоправных целей.

Поэтому реализация защиты медицинской информации в том числе и от киберугроз имеет важное значение.

Сама по себе идея использования блокчейна в здравоохранении не нова, например, в работе Кузнецова В.П. [1], были рассмотрены перспективы и преимущества использования блокчейна в сфере здравоохранения. В свою очередь более детально подобная проблема рассматривалась Пономарёвым К.Ю. [2], однако в работе рассматривается использование облачного хранилища данных, которое тоже может скомпрометировано. В работе Гончаренко Ю.Ю. [3] рассматривается концепт с подтверждением подлинности медицинских документов при помощи технологии блокчейн, однако упускается момент, при котором в некоторых системах необходимо иметь связь с разнородными данными: тексты, числовые значения, графические снимки, которые также должны иметь гарантию подлинности.

По данной тематике существуют коммерческие продукты от компаний BurstIQ, Guardtime и другими [4-8]. Они решают конкретно поставленную за-дачу хранения данных в медицинских информационных системах (МИС). Guardtime использует проприетарный блокчейн, BurstIQ в свою очередь придерживается использования открытых технологий и использует технологию блокчейн для МИС с открытым исходным кодом. В России для Единого депозитария результатов интеллектуальной деятельности (ЕДРИД), Федеральная антимонопольная служба (ФАС) и Сбербанк запустили проект Digital Ecosystem [6-9], где используется технология блокчейн. Проблемы, связанные с использованием МИС в России детально рассматривали Монаков Д.В. и Алтунин Д.В. [7]. Ими выделяется тот факт, что некоторые модули современных МИС зачастую не связаны между собой. Среди востребованных функций внедрение электронных медицинских карт для упрощения работы персонала ЛПУ. Аксенова Е.И. и Гобатов С.Ю. отмечают такие функции как: отслеживание приема лекарств, удаленный мониторинг здоровья, удаленный мониторинг медицинских активов. Однако на основании открытых данных можно сделать вывод, что в большинстве случаев авторы используют просто блокчейн или несколько несвязанных блокчейнов что не позволяет обеспечить хранение разнородных данных.

Прежде, чем предлагать конкретные решения касательно МИС, исполь-зующих блокчейн, надо понимать, что любые значимые данные и обязанности регулируются определенными нормативными актами начиная от конституции РФ заканчивая приказами ФСТЭК России [10-21].

На основании вышеуказанных документов можно определить требования к безопасности систем интернета вещей в сфере здравоохранения:

- Конфиденциальность: только авторизованные пользователи могут получить доступ к данным.
- Целостность: полученные пациентом медицинские данные строго идентичны выданным.
- Аутентификация: процесс, который позволяет медицинскому устройству аутентифицировать и идентифицировать одноранговый узел, с которым оно взаимодействует.
- Доступность: обеспечивает доступность медицинских услуг и устройств Интернета вещей в любое время и в любом месте для авторизованных сторон.
- Неотказуемость: гарантирует, что пользователь или медицинское устройство не сможет отрицать, что является отправителем сообщения.
- Авторизация: гарантирует, что только авторизованная сторона может иметь доступ к данным или иметь разрешение на выполнение определенных задач.

На данный момент в медицинских организациях для осуществления до-машнего стационара преимущественно используются Internet of Medical Things (IoMT) [22]. В таких системах данные о мониторинге пациента передаются в МИС при помощи специальной шины данных. Для передачи данных преимущественно используют такие протоколы, как Message Queuing Telemetry Transport (MQTT), Java Message Service (JMS), eXtensible Messaging and Presence Protocol (XMPP), Advanced Message Queuing Protocol (AMQP), Data Distribution Service (DDS), Constrained Application Protocol (CoAP) [23]. Некоторые из этих протоколов, например, DDS и CoAP, используют UDP, что не гарантирует отправку сообщения что может привести к потере данных при нестабильном соединении, при этом протоколы MQTT, AMQP, XMPP, JMS и при определенной конфигурации DDS используют TCP. Важно отметить, что отправка сообщения не гарантируется, в том случае, когда сервер, на который происходит отправка недо-

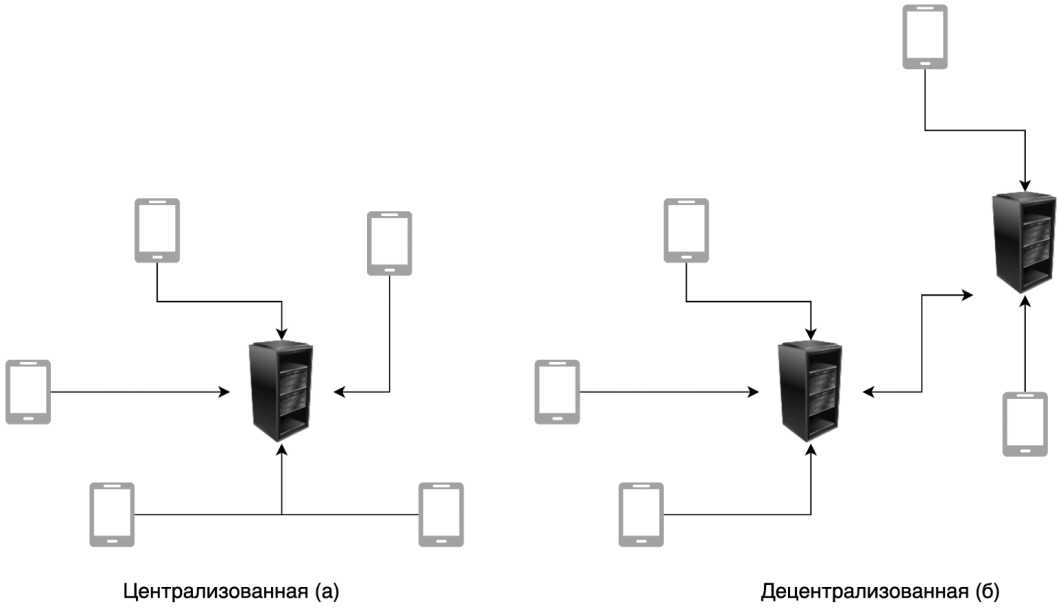


Рис. 1. Подходы к созданию систем. На рисунке (а) архитектура централизованной системы, на рисунке (б) архитектура децентрализованной системы

ступен. Для таких протоколов как CoAP можно использовать несколько серверов для отправки. В этом случае, если один сервер окажется недоступен, будет использован резервный сервер, на который можно отослать данные. Однако разработчикам таких систем необходимо учитывать каким образом сохранять данные для последующего анализа. Определение дублирующих данных также является проблемой, так как данные с IoMT могут прийти в разное время, в зависимости от задержки сети, например, с промежутком в 5 секунд, что может быть критичным.

Существует несколько подходов к созданию систем: централизованный, который применяется в большинстве случаев в МИС, и децентрализованный, они представлены на рис. 1.

Одной из проблем централизованных систем является стоимость, которая необходима для их расширения [24-27], так как в больших информационных системах необходимо тратить дополнительные ресурсы на балансировку нагрузки и синхронизацию баз данных. Распределенные системы могут использовать преимущества централизованной базы данных, особенно при совместном использовании данных. В случае сбоя распределенные системы подвержены меньшему воздействию, чем централизованные, если какой-либо узел в распределенной системе выходит из строя, система не прекратит свое функционирование, так как будут другие узлы для взаимодействия. Топология сети, коммуникационное программное обеспечение и характер распределенных данных являются основными параметрами, влияющими на работу и эффективность распределенной системы. В системе распределенных баз данных используются сложные методы управления данными для решения проблем, связанных с целостностью данных и параллелизмом. Поскольку данные расположены и репли-цируются в разных местах, то это может привести к несогласованности данных при каждом изменении данных в определенном месте.

Блокчейн – это технология, которая позволяет записывать и обмениваться общими данными по распределенной сети. Данные хранятся в неизменяемых "блоках", которые последовательно соединены друг с другом. Каждый блок содержит свой собственный хэш и хэш предыдущего блока, что обеспечивает целостность данных. Блокчейн масштабируем и обладает такой же децентрализацией, как и IoT. Существуют различные типы блокчейнов:

• Публичный – блокчейн, к которому может присоединиться любой пользователь. Он может считывать данные, обновлять и записывать новые, что позволяет публичному

блокчейну сохранять свой самоуправляемый характер. Недостатком являются высокие энергозатраты при увеличении числа участников.

• Приватный блокчейн, допускаются только верифицированные участ-ники с авторизацией или подтвержденным приглашением. Это позволяет использовать согласованный протокол и вести общий реестр.

• Блокчейн на основе разрешений – комбинация публичного и частного блокчейнов с возможностью дальнейшей настройки ролей.

Медицинские приложения требуют взаимодействия только с идентифи-цированными и прошедшими аутентификацию устройствами. Подходит как приватный блокчейн, так и блокчейн, основанный на разрешениях.

Смарт контракт является одним из ключевых инновационных элементов технологии блокчейн. Он представляет собой программный код, который выполняются автоматически при определенных условий, описанных в контракте. Смарт контракты обеспечивают автоматизацию и безопасность сделок без участия посредников. В здравоохранении смарт контракты могут повысить и эффективность, и прозрачность процессов в сфере медицинских услуг и управления медицинскими данными. Например, с помощью смарт контрактов можно автоматизировать процессы страхования здоровья, управления медицинскими досье и рецептами, а также оплаты медицинских услуг. Одним из примеров использования смарт контрактов в здравоохранении, может быть, система управления медицинскими данными пациентов. С помощью смарт контрактов можно создать защищенную и прозрачную цифровую базу данных, в которой будут храниться медицинские записи пациентов. Доступ к этим данным можно предоставлять только авторизованным лицам, что обеспечит конфиденциальность информации.

Кроме того, смарт контракты могут упростить процессы взаимодействия между различными участниками системы здравоохранения, такими как пациенты, врачи, страховые компании и административные органы. Например, с помощью смарт контрактов можно автоматизировать процесс оплаты медицинских услуг между страховыми компаниями и медицинскими учреждениями на основе предоставленных данных о выполненных процедурах и лечении. Поскольку данные поступают в режиме реального времени, смарт контракты могут автоматически обновлять отчеты и справки о состоянии здоровья. Это особенно полезно для хронически больных пациентов, которым необходимо регулярное обновление данных для корректировки лечения. Длительность разработки смарт контрактов зависит от требований, чем они сложнее, тем дольше придется разрабатывать смарт контракт, а также от того какая база блокчейна используется, является ли это уже закрепившимся решением, таким как Etherium или это что-то оригинальное.

Таким образом, смарт контракты имеют огромный потенциал для улуч-шения качества и доступности здравоохранения. Их внедрение может способствовать повышению эффективности процессов, снижению издержек и улуч-шению качества медицинского обслуживания, за счет упрощения коллаборации, с научно-исследовательскими институтами, создании персональных пла-нов лечения. В будущем использование смарт контрактов в здравоохранении может стать стандартной практикой, что приведет к созданию более эффективной и безопасной системы здравоохранения.

Стоит обратить внимание, что для обработки потоковых данных (например, данных ЭКГ) для блокчейна требуются дополнительные модификации, которые позволяют работать с цепочками одновременных данных от одного пациента. Такой подход позволяет предоставлять определенные данные в отдельных цепочках в общем потоке.

Блокчейн предлагается использовать для дублирования данных из базы данных, если такая база уже есть у МИС. Использование блокчейна позволяет хранить данные в облачном хранилище провайдера, а также обеспечить уско-рение процессов взаимодействия и принятия решений. В условиях домашнего стационара оперативное взаимодействие между пациентами, врачами и другими участниками системы крайне важно. Блокчейн может значительно ускорить обмен данными и принятие решений за счет автоматизации процессов через смартконтракты. Например, когда состояние пациента меняется, соответствующие данные могут быть автоматически переданы врачу для немедленного анализа и корректировки лечения. Кроме того, смартконтракты могут быть использованы для автоматизации процедур страхования, обеспечивая быстрое и точное возмещение затрат на медицинские услуги. Также это позволяет обеспечить поддержку интероперe-

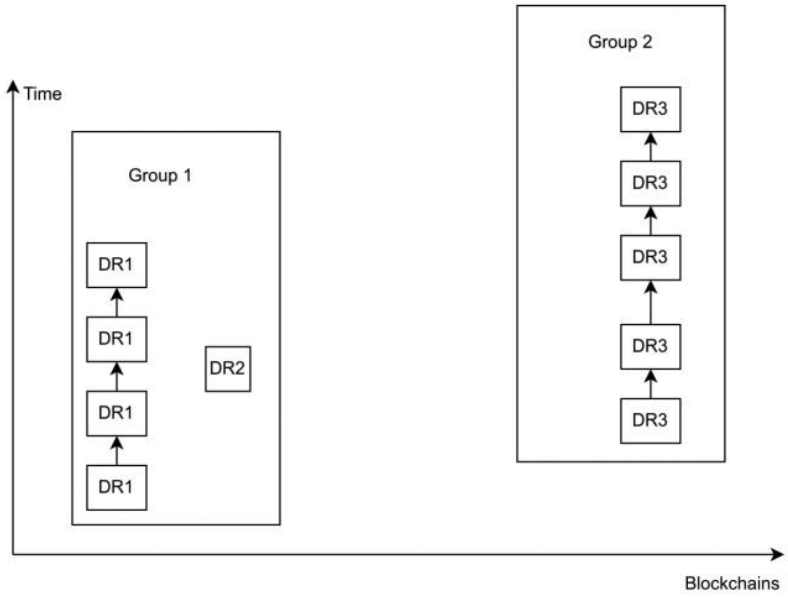


Рис. 2. Архитектура хранения данных в блокчейне

рабельности и стандартизации данных, так как медицинские данные, поступающие из различных устройств и систем, часто имеют разнородные форматы и стандарты. Это особенно актуально для домашнего стационара, где данные могут поступать от различных производителей медицинских устройств. Блокчейн позволяет унифицировать процесс сбора и обработки данных, что упрощает их интеграцию и последующий анализ. В результате врачи получают доступ к более точной и структурированной информации, что способствует повышению качества лечения.

Для хранения данных предлагается использовать блокчейн-блокчейнов, где в каждом блокчейне будут храниться данные по каждому пациенту, таким образом увеличивая консистентность данных. Схема хранения данных представлена на рис. 2.

На рис. 3 представлена архитектурная схема МИС с использованием блокчейн. На схеме, мобильные устройства отражают устройства, используемые в рамках домашнего стационара, они передают данные в блокчейн в свою медицинскую организацию. Архитектура состоит из нескольких каналов связи (Channel 1, Channel 2, Channel 3 и других), каждый из которых объединяет несколько блокчейн-менеджеров, которые привязаны к определенным медицинским учреждениям, которые объединены в единую сеть для обмена информацией между собой. Блокчейн-менеджеры представляют собой узлы, ответственные за управление блокчейнами и обеспечивающие взаимодействие с данными.

В контексте телемедицинских технологий, такая архитектура позволяет безопасно и эффективно управлять медицинскими данными пациентов. Каждый канал может быть выделен для определенного набора медицинских учреждений или групп пациентов, что позволяет обеспечить гибкость и адаптируемость системы к различным условиям.

В домашних стационарах такая архитектура обеспечивает безопасное хранение данных о состоянии здоровья пациентов, доступных в режиме реального времени для медицинских работников. Блокчейн-менеджеры, работающие в рамках своих каналов, гарантируют неизменность и подлинность данных. Совет – это группа избранных или назначенных участников, которые управляют сетью или принимают ключевые решения по развитию и функционированию блокчейна, обеспечивает координацию между всеми участниками системы.

Отметим, что одним из вариантов внедрения технологий, использующих блокчейн, может быть создание дополнительной инфраструктуры на основе блокчейн в качестве дублирующей базы МИС, например, для домашнего стационара. С одной стороны, для этого не требуется дополнительных изменений. В используемую МИС достаточно непосредственно для базы данных МИС разработать триггер, отправляющий данные в блок-

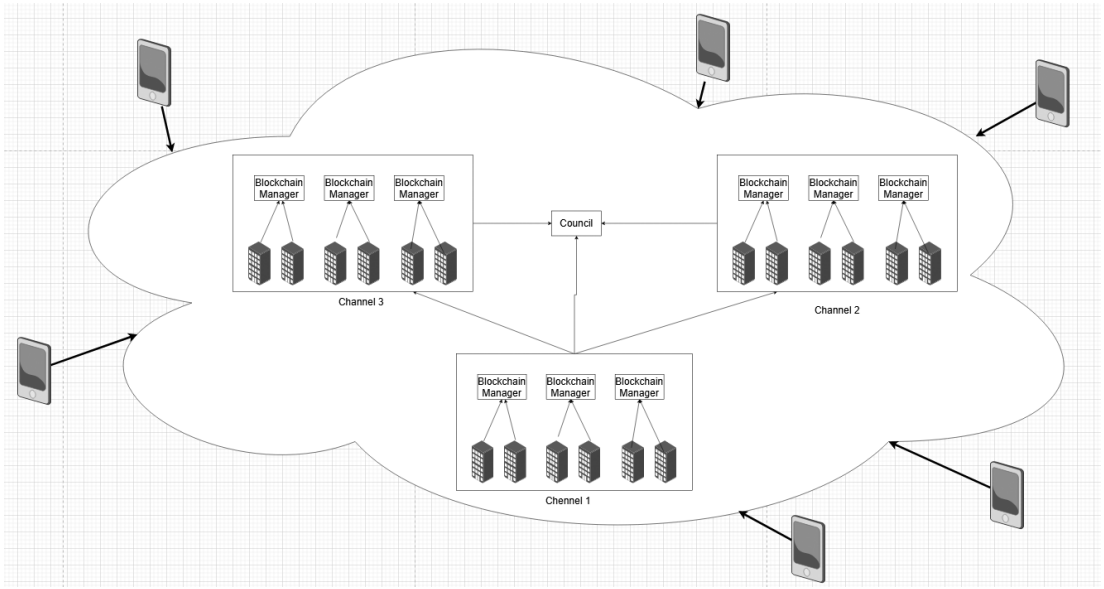


Рис. 3. Предлагаемая архитектурная схема для использования в существующих МИС

чейн, в дополнение к основной базе, или специальный шедулер, который направляет эти данные по расписанию. В условиях домашнего стационара оперативное взаимодействие между пациентами, врачами и другими участниками системы крайне важно. Блокчейн может значительно ускорить обмен данными для принятия решений за счет автоматизации процессов через смарт-контракты. Например, когда состояние пациента меняется, соответствующие данные могут быть автоматически переданы врачу для немедленного анализа и корректировки лечения. Кроме того, смарт-контракты могут быть использованы для автоматизации процедур страхования, обеспечивая быстрое и точное возмещение затрат на медицинские услуги. Также в медицинской информационной системе домашнего стационара прозрачность данных играют важную роль в обеспечении качественного медицинского обслуживания. Блокчейн позволяет каждому участнику системы (врачам, пациентам, страховым компаниям и другим заинтересованным сторонам) иметь доступ к полному журналу транзакций и изменений в данных. Это не только увеличивает доверие к системе, но и позволяет быстро и точно отслеживать любую информацию, необходимую для принятия медицинских решений. Такая прозрачность также помогает в решении спорных ситуаций, связанных и с диагнозом, и с лечением пациента.

Для получения информации, хранимой в блокчейне, необходим API, к которому были выдвинуты следующие требования:

1) поддержка основных операций блокчейна: API должен поддержи-вать основные операции, такие как создание транзакций, чтение и запись дан-ных, валидация транзакций и доступ к информации о блоках и их содержимому;

2) работа со смарт-контрактами: возможность развертывания и вызова смарт-контрактов, а также взаимодействия с ними;

3) управление учетными записями: создание и проверка статуса учетных записей (адресов) пользователей, управление пользователями;

4) доступ к истории транзакций: возможность получения полной истории транзакций для конкретной учетной записи.

Также стоит упомянуть, что в зависимости от сложности запроса, можно воспользоваться как стандартным API блокчейна, так и смарт-контрактом, так как они предлагают более гибкую выборку данных.

Для пользовательского интерфейса доступа к данным, хранящимся в блокчейне, также были определены требования, обусловленные в том числе выбором целевой аудитории пользователей технологии – медицинских работников:

1) необязательность ручного ввода;
2) низкий порог обучения для применения;
3) безопасность конфиденциальных данных.

Один из вариантов интерфейса, удовлетворяющего данным требованиям, – голосовое управление посредством виртуального ассистента [28]. Голосовой ввод команд позволяет врачу получать информацию из базы данных, не отрываясь от работы с пациентом, что, согласно [29], снижает риск случайного занесения инфекций, упрощает круг обязанностей ассистирующего врача и улучшает опыт посещения врача пациентами. Использование технологий обработки естественного языка для ввода голосовых команд упрощает процесс обучения пользователей системы, фокусируясь на функциональных возможностях виртуального ассистента без необходимости заучивать формальные команды. Безопасность использования системы голосового помощника предлагается достичь внедрением системы непрерывной аутентификации врача-пользователя [30].

Для иллюстрации взаимодействия медицинского работника с API приве-дем некоторые примеры пользовательских запросов:

• запрос на получение истории посещений клиник: GET /getHospitalVisits, с параметром идентификатора пациента;

• запрос на получение документов по пациенту из конкретной клиники: GET / getDocumentsFromHospital, с параметром идентификатора мед. учреждения, полученного из пункта 1 и идентификатора пациента;

• запрос на получение конкретного документа: GET /getDocument, с параметром идентификатора документа, полученного из пункта 2.

Ниже предоставлен пример листинга 1, в котором происходит обработка запроса на получение истории посещений клиник.

Листинг 1 – Пример кода смарт-контракта на языке Solidity по запросу на получение истории посещений клиник

```
   pragma solidity ^0.8.0;
   contract HospitalVisits {
       struct HospitalVisit {
           string hospitalName;
           string department;
           uint256 visitDate; // Unix timestamp of the visit
           string reasonForVisit;
       }
       mapping(address => HospitalVisit[]) private hospitalVisits;
       event VisitAdded(address indexed patient, string hospitalName,
uint256 visitDate);
       function addHospitalVisit(
           string memory _hospitalName,
           string memory _department,
           uint256 _visitDate,
           string memory _reasonForVisit
       ) public {
           HospitalVisit memory newVisit = HospitalVisit({
               hospitalName: _hospitalName,
               department: _department,
               visitDate: _visitDate,
               reasonForVisit: _reasonForVisit
           });
           hospitalVisits[msg.sender].push(newVisit);
           emit VisitAdded(msg.sender, _hospitalName, _visitDate);
       }
       function getHospitalVisits() public view returns (HospitalVisit[]
memory) {
           return hospitalVisits[msg.sender];
       }
       function getPatientHospitalVisits(address patient) public view
returns (HospitalVisit[] memory) {
           return hospitalVisits[patient];
       }
   }
```

**Заключение**

В данной статье предложен инновационный подход к интеграции техно-логии блокчейн с медицинскими информационными системами (МИС), работающими с устройствами Интернета медицинских вещей (IoMT), для улучшения качества и безопасности медицинских данных. Использование блокчейна обеспечивает создание распределенного и защищенного хранилища данных, что особенно актуально для домашних стационаров и медицинских учреждений. Это решение позволяет улучшить управление медицинскими данными, обеспечить их конфиденциальность и целостность, а также значительно ускорить процессы принятия решений.

Кроме того, предложенная архитектура позволяет использовать смарт-контракты для автоматизации различных процессов, включая страхование и корректировку лечения на основе реальных данных пациента. Это открывает новые возможности для взаимодействия медицинских учреждений, врачей и пациентов, а также улучшает прозрачность и надежность хранения данных.

Таким образом, использование технологии блокчейн в контексте МИС и IoMT является перспективным направлением для дальнейшего развития здравоохранения, которое поможет повысить эффективность и безопасность медицинских услуг.

**Литература**


1. Кузнецова В. П., Вардомацкая Л. П., Тропинова Е. А. Блокчейн в зда-воохранении // Экономика и управление. 2018. No 7 (153). С. 16–20.

2. Гончаренко, Ю. Ю. Использование технологии блокчейн для проверки подлинности электронных документов и файлов / Ю. Ю. Гончаренко // БЛОКЧЕЙН — 2023 г. — № 1 (47) — С. 98-101

3. Захаров, А. А. Методы разграничения доступа в сетях интернета медицинских вещей на основе атрибутивных моделей 1 / А. А. Захаров, К. Ю. Пономарёв // Телемедицина — 2020 г. — № 4 (38) — С. 44-54

4. W. A. N. A. Al-Nbhany, A. T. Zahary and A. A. Al-Shargabi, "Blockchain-IoT Healthcare Applications and Trends: A Review," // IEEE Access, vol. 12, pp. 4178-4212, 2024

5. Litvin, A. A. The Possibilities of Blockchain Technology in Medicine (Re-view) / A. A. Litvin, S. V. Korenev, E. G. Knyazeva, V. Litvin // БЛОКЧЕЙН — 2019 г. — № 4 — С. 191-199

6. Сбербанк и ФАС России запустили пилотный проект по обмену доку-ментами на основе Blockchain [Электронный ресурс] / Сбербанк крупнейший транснациональный и универсальный банк России, Центральной и Восточной Европы. — Режим доступа: https://www.sberbank.ru/ru/press_center/a11/artic1e?newsID=cb85f87f-8дc4-46df-8fdf-eab909д0277c& block-ID=1303& regionID=&1ang=ru (дата обращения: 16.05.2024).

7. Монаков, Д. М. Медицинские информационные системы: современные реалии и перспективы / Д. М. Монаков, Д. В. Алтунин // МИС — 2022 г. — № 4 — С. 46-53.

8. Аксенова Е. И., Горбатов С. Ю. Интернет медицинских вещей (IoMT): новые возможности для здравоохранения //М.: НИИОЗММ ДЗМ. – 2021.

9. Шадёркин И. А. и др. Информационные технологии в организации домашнего стационара для людей с ограниченными возможностями //Журнал телемедицины и электронного здравоохранения. – 2018. – №. 3 (8). – С. 57-63.

10. Конституция Российской Федерации: [принята всенародным голосо-ванием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01 июля 2020 г.]. – Текст: электронный // Официальный интернет–портал правовой информации. – URL: http://www.pravo.gov.ru (дата обращения: 22.01.2024).

11. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ // СПС Консультант Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 22.01.2024).

12. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, ин-формационных технологиях и о защите информации» // СПС Консультант Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 22.01.2024).

13. Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в РФ» // СПС Консультант Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_121895/ (дата обращения 22.01.2024).

14. Приказ ФСТЭК от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // ФСТЭК России URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения 22.01.2024).

15. Приказ Минздрава России от 24.12.2018 N 911н "Об утверждении Требований к государственным информационным системам в сфере здраво-охранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацев-тических организаций" // СПС Консультант Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_327147/ (дата обращения 22.01.2024).

16. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утвер-ждении требований к защите персональных данных при их обработке в информационных системах персональных данных" // СПС Консультант Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_137356/ (дата обращения 22.01.2024).

17. Приказ Минздрава России от 30.11.2017 N 965н "Об утверждении порядка организации и оказания медицинской помощи с применением телемедицинских технологий" // СПС Консультант Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_287515/ (дата обращения 22.01.2024).

18. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ // СПС Кон-сультант Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_287515/ (дата обращения 22.01.2024).

19. Постановление Правительства РФ от 08.02.2018 N 127 (ред. от 20.12.2022) "Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений" // СПС Консультант Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_290595/249cdc5b469dbd358edc05698e5b3e4be012269a/#dst100074 (дата обращения 22.01.2024).

20. Приказ ФСТЭК от 25 декабря 2017 г. N 239 "Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации" // ФСТЭК России URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения 22.01.2024).

21. Приказ ФСТЭК от 21 декабря 2017 г. N 235 "Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечению их функционирования" // ФСТЭК России URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235 (дата обраще-ния 22.01.2024).

22. Информационные технологии в организации домашнего стационара для людей с ограниченными возможностями / И. А. Шадёркин, Г. С. Лебедев, А. В. Владзимирский, А. А. Лисненко и др. // СТАЦИОНАР НА ДОМУ — 2018 г. — № 3 (8) — С. 57-63.

23. Ruzmetov A., Khudaybergenov T. Survey of IoT application layer proto-cols //Modern Science and Research. – 2024. – Т. 3. – №. 1. – С. 1-5.

24. Vidyarthi D. P. et al. Scheduling in distributed computing systems: Analysis, design and models. – Springer Science & Business Media, 2008.

25. Mesbahi M., Rahmani A. M. Load balancing in cloud computing: a state of the art survey //Int. J. Mod. Educ. Comput. Sci. – 2016. – Т. 8. – №. 3. – С. 64.

26. Patki T. et al. Economic viability of hardware overprovisioning in power-constrained high performance computing //2016 4th International Workshop on Energy Efficient Supercomputing (E2SC). – IEEE, 2016. – С. 8-15.

27. Gupta A. et al. The who, what, why, and how of high performance computing in the cloud //2013 IEEE 5th international conference on cloud computing technology and science. – IEEE, 2013. – Т. 1. – С. 306-314.

28. Применение голосового помощника в качестве виртуального консультанта для администрирования безопасности инфраструктуры локальной компьютерной сети / А. А. Захаров, А. М. Шабалин, Ш. И. Ханбеков, Д. Б. Джалилзода и др. // Виртуальный голосовой помощник — 2022 г. — № 4 (46) — С. 68-75.

29. Warren S. et al. Acceptance of voice assistant technology in dental prac-tice: A cross sectional study with dentists and validation using structural equation modeling //PLOS Digital Health. – 2024. – Т. 3. – №. 5. – С. e0000510.

30. Khanbekov S., Zakharov A. Continuous speaker authentication when using network administrator virtual assistant //2023 International Russian Smart Industry Conference (SmartIndustryCon). – IEEE, 2023. – С. 202-206.

## References


1. Kuznetsova V. P., Vardomatskaya L. P., Tropinova Ye. A. Blokcheyn v zdavookhranenii // Ekonomika i upravleniye. 2018. No 7 (153). S. 16–20.

2. Goncharenko, YU. YU. Ispol'zovaniye tekhnologii blokcheyn dlya pro-verki podlinnosti elektronnykh dokumentov i faylov / YU. YU. Goncharenko // BLOKCHEYN — 2023 g. — № 1 (47) — S. 98-101

3. Zakharov, A. A. Metody razgranicheniya dostupa v setyakh interneta me-ditsinskikh veshchey na osnove atributivnykh modeley 1 / A. A. Zakharov, K. YU. Ponomarov // Telemeditsina — 2020 g. — № 4 (38) — S. 44-54.

4. U. A. N. A. Al-Nbhani, A. T. Zahari and A. A. Al-Sharghabi, "Blockchain applications and trends of the Internet of Things in healthcare: an overview" // IEEE Access, volume 12, pp. 4178-4212, 2024

5. Litvin, A. A. The possibilities of blockchain technology in medicine (Re-view) / A. A. Litvin, S. V. Korenev, E. G. Knyazeva, V. Litvin // BLOCKCHAIN — 2019 — No. 4 — pp. 191-199

6. Sberbank i FAS Rossii zapustili pilotnyy proyekt po obmenu do-kumentami na osnove Blockchain [Elektronnyy resurs] / Sberbank krupney-shiy transnatsional'nyy i universal'nyy bank Rossii, Tsentral'noy i Vo-stochnoy Yevropy. — Rezhim dostupa: https://www.sberbank.ri/gi/press_center/a11/artic1e?newsID=cb85f87f-8dc4-46df-8fdf-eab909d0277c& Yosk-ID=1303& regionID=&1ang=ru (data obrashche-niya: 16.05.2024).

7. Monakov, D. M. Meditsinskiye informatsionnyye sistemy: sovremen-nyye realii i perspektivy / D. M. Monakov, D. V. Altunin // MIS — 2022 g. — № 4 — S. 46-53.

8. Aksenova Ye. I., Gorbatov S. YU. Internet meditsinskikh veshchey (IoMT): novyye vozmozhnosti dlya zdravookhraneniya //M.: NIIOZMM DZM. – 2021.

9. Shadorkin I. A. i dr. Informatsionnyye tekhnologii v organizatsii domashnego statsionara dlya lyudey s ogranichennymi vozmozhnostyami //Zhurnal telemeditsiny i elektronnogo zdravookhraneniya. – 2018. – №. 3 (8). – S. 57-63.

10. Konstitutsiya Rossiyskoy Federatsii: [prinyata vsenarodnym golo-sovaniyem 12 dekabrya 1993 g. s izmeneniyami, odobrennymi v khode obshcheros-siyskogo golosovaniya 01 iyulya 2020 g.]. – Tekst: elektronnyy // Ofitsial'-nyy internet–portal pravovoy informatsii. – URL: http://www.pravo.gov.ru (data obrashcheniya: 22.01.2024).

11. Federal'nyy zakon "O personal'nykh dannykh" ot 27.07.2006 N 152-FZ // SPS Konsul'tant Plyus URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (data obrashcheniya 22.01.2024).

12. Federal'nyy zakon ot 27.07.2006 № 149-FZ «Ob informatsii, in-formatsionnykh tekhnologiyakh i o zashchite informatsii» // SPS Konsul'tant Plyus URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (data obrashcheniya 22.01.2024).

13. Federal'nyy zakon ot 21.11.2011 № 323-FZ «Ob osnovakh okhrany zdo-rov'ya grazhdan v RF» // SPS Konsul'tant Plyus URL: https://www.consultant.ru/document/cons_doc_LAW_121895/ (data obrashcheniya 22.01.2024).

14. Prikaz FSTEK ot 18 fevralya 2013 g. N 21 «Ob utverzhdenii so-stava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh» // FSTEK Rossii URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (data obrashcheniya 22.01.2024).

15. Prikaz Minzdrava Rossii ot 24.12.2018 N 911n "Ob utverzhdenii Trebovaniy k gosudarstvennym informatsionnym sistemam v sfere zdravo-okhraneniya sub"yektov Rossiyskoy Federatsii, meditsinskim informatsionnym sistemam meditsinskikh organizatsiy i informatsionnym sistemam farmatsev-ticheskikh organizatsiy" // SPS Konsul'tant Plyus URL: https://www.consultant.ru/document/cons_doc_LAW_327147/ (data obrashcheniya 22.01.2024).

16. Postanovleniye Pravitel'stva RF ot 01.11.2012 N 1119 "Ob utver-zhdenii trebovaniy k zashchite personal'nykh dannykh pri ikh obrabotke v in-formatsionnykh sistemakh personal'nykh dannykh" // SPS Konsul'tant Plyus URL: https://www.consultant.ru/document/cons_doc_LAW_137356/ (data ob-rashcheniya 22.01.2024).

17. Prikaz Minzdrava Rossii ot 30.11.2017 N 965n "Ob utverzhdenii poryadka organizatsii i okazaniya meditsinskoy pomoshchi s primeneniyem tele-meditsinskikh tekhnologiy" // SPS Konsul'tant Plyus URL: https://www.consultant.ru/document/cons_doc_LAW_287515/ (data obrashcheniya 22.01.2024).

18. Federal'nyy zakon "O bezopasnosti kriticheskoy informatsionnoy infra-struktury Rossiyskoy Federatsii" ot 26.07.2017 N 187-FZ // SPS Konsul'tant Plyus URL: https://www.consultant.ru/document/cons_doc_LAW_287515/ (data obrash-cheniya 22.01.2024).

19. Postanovleniye Pravitel'stva RF ot 08.02.2018 N 127 (red. ot 20.12.2022) "Ob utverzhdenii Pravil kategorirovaniya ob"yektov kritiche-skoy informatsionnoy infrastruktury Rossiyskoy Federatsii, a takzhe pe-rechnya pokazateley kriteriyev znachimosti ob"yektov kriticheskoy informatsi-onnoy infrastruktury

Rossiyskoy Federatsii i ikh znacheniy" // SPS Kon-sul'tant Plyus URL: https://www.consultant.ru/document/cons_doc_LAW_290595/249cdc5b469dbd358edc05698e5b3e4be012269a/#dst100074 (data obrashcheniya 22.01.2024).

20. Prikaz FSTEK ot 25 dekabrya 2017 g. N 239 "Ob utverzhdenii tre-bovaniy po obespecheniyu bezopasnosti znachimykh ob"yektov kriticheskoy in-formatsionnoy infrastruktury rossiyskoy federatsii" // FSTEK Rossii URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (data obrashcheniya 22.01.2024).

21. Prikaz FSTEK ot 21 dekabrya 2017 g. N 235 "Ob utverzhdenii tre-bovaniy k sozdaniyu sistem bezopasnosti znachimykh ob"yektov kriticheskoy informatsionnoy infrastruktury rossiyskoy federatsii i obespecheniyu ikh funktsionirovaniya" // FSTEK Rossii URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235 (data ob-rashcheniya 22.01.2024).

22. Informatsionnyye tekhnologii v organizatsii domashnego statsiona-ra dlya lyudey s ogranichennymi vozmozhnostyami / I. A. Shadorkin, G. S. Le-bedev, A. V. Vladzimirskiy, A. A. Lisnenko i dr. // STATSIONAR NA DO-MU — 2018 g. — № 3 (8) — S. 57-63.

23. Ruzmetov A., Khudaybergenov T. Survey of IoT application layer pro-tocols //Modern Science and Research. – 2024. – T. 3. – №. 1. – S. 1-5.

24. Vidyarthi D. P. et al. Scheduling in distributed computing systems: Analysis, design and models. – Springer Science & Business Media, 2008.

25. Mesbahi M., Rahmani A. M. Load balancing in cloud computing: a state of the art survey //Int. J. Mod. Educ. Comput. Sci. – 2016. – T. 8. – №. 3. – S. 64.

26. Patki T. et al. Economic viability of hardware overprovisioning in power-constrained high performance computing //2016 4th International Work-shop on Energy Efficient Supercomputing (E2SC). – IEEE, 2016. – S. 8-15.

27. Gupta A. et al. The who, what, why, and how of high performance computing in the cloud //2013 IEEE 5th international conference on cloud com-puting technology and science. – IEEE, 2013. – T. 1. – S. 306-314.

28. Primeneniye golosovogo pomoshchnika v kachestve virtual'nogo kon-sul'tanta dlya administrirovaniya bezopasnosti infrastruktury lokal'noy komp'yuter-noy seti / A. A. Zakharov, A. M. Shabalin, SH. I. Khanbekov, D. B. Dzhalilzoda i dr. // Virtual'nyy golosovoy pomoshchnik — 2022 g. — № 4 (46) — S. 68-75.

29. Warren S. et al. Acceptance of voice assistant technology in dental prac-tice: A cross sectional study with dentists and validation using structural equation modeling //PLOS Digital Health. – 2024. – T. 3. – №. 5. – S. e0000510.

30. Khanbekov S., Zakharov A. Continuous speaker authentication when using network administrator virtual assistant //2023 International Russian Smart Industry Conference (SmartIndustryCon). – IEEE, 2023. – S. 202-206.

---

**КОРЕНЕВ Дмитрий Александрович,** аспирант кафедры «Информаци-онной безопасности», Тюменский государственный университет. 625003, г. Тюмень, ул. Володарского, 6. E-mail: koreneffdmitrii@gmail.com

**ХАНБЕКОВ Шамиль Ирекович,** аспирант кафедры «Информационной безопасности», Тюменский государственный университет. 625003, г. Тюмень, ул. Володарского, 6. E-mail: s.i.khanbekov@utmn.ru

**ЗАХАРОВ Александр Анатольевич,** доктор технических наук, заве-дующий базовой кафедрой «Безопасные ИТ умного города», Тюменский государственный университет. 625003, г. Тюмень, ул. Володарского, 6. E-mail: a.a.zakharov@utmn.ru

**KORENEV Dmitry Alexandrovich,** Postgraduate student of the Department of Information Security, Tyumen State University. 625003, Tyumen, Volodarsky st., 6. E-mail: koreneffdmitrii@gmail.com

**KHANBEKOV Shamil Irekovich,** Postgraduate student of the Department of Information Security, Tyumen State University. 625003, Tyumen, Volodarsky st., 6. E-mail: s.i.khanbekov@utmn.ru

**ZAKHAROV Alexander Alexandrovich,** Doctor of Technical Sciences, Head of the Basic Department of "Secure IT of a Smart City", Tyumen State University. 625003, Tyumen, Volodarsky st., 6. E-mail: a.a.zakharov@utmn.ru

УДК 004.94 Вестник УрФО № 3(53) / 2024, с. 26–31

**Воробьев А. П., Кротова Е. Л., Воробьева Е. Ю.** DOI: 10.14529/secur240303

# *ИСПОЛЬЗОВАНИЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ ДЛЯ ОБМЕНА КЛЮЧАМИ В IOT*

*Статья посвящена основам криптографии на эллиптических кривых, проведен анализ преимущества использования ECDLP алгоритмов для IoT устройств. Был исследован алгоритм обмена ключами ECDH, применимый для IoT. При использовании кривой Curve25519 построен метод обмена ключами X25519. Данный алгоритм обеспечивает 128-битный уровень защиты, что соответствует уровню симметричного шифрования AES-128, который может использоваться после обмена ключами.*

***Ключевые слова:*** *криптография, эллиптические кривые, обмен ключами в IoT устройствах.*

**Vorobev A. P., Krotova E. L., Vorobeva E. Yu.**

# *USING ELLIPTIC CURVES FOR KEY EXCHANGE IN IOT*

*The article is devoted to the basics of elliptic curve cryptography and analyzes the advantages of using ECDLP algorithms for IoT devices. The ECDH key exchange algorithm applicable to IoT was investigated. Using Curve25519, the X25519 key exchange method has been built. This algorithm provides a 128-bit security level, which corresponds to the AES-128 symmetric encryption level that can be used after key exchange.*

***Keywords:*** *cryptography, elliptic curves, key exchange in IoT devices.*

Интернет вещей (IoT) – это концепция сети, в которой физические объекты обмениваются данными через Интернет, без необходимости прямого вмешательства человека. IoT представляет собой систему взаимодействия между физическими устройствами, работающими с помощью встроенных датчиков и программного обеспечения для обмена данными через интернет. Использование IoT предполагается в различных отраслях, начиная от носимых устройств и умного дома, до промышленного оборудования в рамках концепции умного предприятия.

Согласно анализу IoT Analytics, к 2027 году число подключений к Интернету вещей, вероятно, превысит 29 миллиардов [1]. Однако, одним из основных недостатков IoT является проблема безопасности подключения. Подключенные устройства IoT могут стать объектом взлома, и злоумышленники могут получить доступ к чувствительным данным или даже контролировать эти устройства. Поэтому с ростом количества устройств Интернета вещей вопрос эффективной защиты становится ключевым в развитии этой технологии: безопасность играет важную роль в разработке, установке и эксплуатации сетей IoT.

В данном контексте необходимо обратить внимание на применение современных методов криптографии для обеспечения безопасности передачи данных в IoT сетях.

*Причины применения криптографии для Iot устройств на эллиптических кривых*

Устройства IoT имеют ограниченные функциональные возможности, которые характеризуются меньшим объемом памяти и вычислительной мощности, чем обычные устройства [2]. Криптография на эллиптических кривых может стать лучшим решением для таких устройств, так как алгоритмы на эллиптических кривых имеют существенно меньшую длину ключа при равной стойкости [3]. Алгоритмы, основанные на проблеме дискретного логарифмирования (DLP – Discrete Logarithm Problem), имеют больший ключ, чем алгоритмы с проблемой дискретного логарифмирования на эллиптических кривых (ECDLP – Elliptic Curve Discrete Logarithm Problem). Например, 2028 бит для алгоритма Диффи-Хеллмана и 256 бит для Диффи-Хеллмана на эллиптических кривых.

При увеличении вычислительных мощностей растет и вероятность взлома алгоритмов, что влечет за собой необходимость увеличивать длину ключа для обеспечения достаточного уровня защиты. Например, до 1 октября 2015 года 1024-разрядные ключи RSA были разрешены для использования, сейчас настоятельно рекомендуется использовать 2048-разрядные ключи RSA [4].

Также при увеличении уровня защиты длина ключей DLP алгоритмов и ECDLP алгоритмов увеличивается непропорционально. Например, при увеличении ключа DH в два раза (с 1024 до 2048 бит) аналогичный алгоритм на эллиптических кривых ECDH увеличивает длину в 1,4 раза (с 160 до 224 бит). Сравнение алгоритмов по длине ключа приведено в таблице 1 [5].

Таким образом, при дальнейшем использовании и увеличении уровня защиты ECDLP алгоритмы будут эффективнее использовать память устройства. Данное свойство может быть крайне полезно для IoT устройств.

*Протоколы с использованием эллиптических кривых*

Пусть задано конечное простое поле $F_p$, характеристика которого $p > 3$. Пусть кривая $E$, заданная уравнением

$$E : y^2 \equiv x^3 + ax + b \pmod{p}, \qquad (1)$$

определена над полем $F_p$ и точка $P \in E(F_p), P \neq O$. Здесь $O$ – точка на бесконечности (нейтральный, нулевой элемент) [6].

При этом кривая (1) является несингулярной, т. е. ее дискриминант

$$\Delta(E) = 4a^3 + 27b^2 \neq 0 \pmod{p}.$$

$n$-кратным точки $P$ назовем композицию (сумму):

$$[n]P = \underbrace{P + P + \ldots + P}_{n \text{ раз}}.$$

Наименьшее натуральное число $n$ такое, что $[n]P = O$, называется порядком $P$ в группе $E(F_p)$. Количество точек кривой $E$ будем обозначать $N$.

*Таблица 1.*

**Сравнение алгоритмов по длине ключа.**

| Уровень защиты | Алгоритм симметричного шифрования | DSA, DH (L – открытый ключ, N – закрытый ключ), бит | RSA (k – длина ключа), бит | ECDSA, EdDSA, ECDH (f – длина ключа), бит |
|---|---|---|---|---|
| ≤ 80 | 2TDEA | L = 1024<br>N = 160 | k = 1024 | f = 160-223 |
| 112 | 3TDEA | L = 2048<br>N = 224 | k = 2048 | f = 224-255 |
| 128 | AES-128 | L = 3072<br>N = 256 | k = 3072 | f = 256-383 |
| 192 | AES-192 | L = 7680<br>N = 384 | k = 7680 | f = 384-511 |
| 256 | AES-256 | L = 15360<br>N = 512 | k = 15360 | f = 512+ |

Для задания эллиптической кривой согласно национальному стандарту РФ (ГОСТ Р 34.10-2012) необходимо определить следующие параметры [7]:

$p$ – простое число, модуль эллиптической кривой $(p>3)$, задающее размер конечного поля;

$a, b$ – коэффициенты уравнения (1);

$P$ – порождающая точка, или генератор точек кривой, точка большого порядка $q$. При $1 \le m \le q-1$ последовательность $\{[m]P\}$ задает все различные точки кривой, $[q]P = O$;

$q$ – порядок точки $P$ или порядок подгрупп; $2^{254} < q < 2^{256}$ или $2^{508} < q < 2^{512}$;

$h = \frac{N}{q}$ – кофактор кривой (подгруппы) [8].

*Алгоритм ECDSA*

Алгоритм цифровой подписи на эллиптической кривой – это криптографически защищенная схема цифровой подписи, основанная на криптографии с эллиптической кривой (ECC). Алгоритм подтверждения цифровой подписи ECDSA (Elliptic Curve Digital Signature Algorithm) основан на умножении точек эллиптической кривой.

Ключи и подписи ECDSA короче, чем в RSA, для того же уровня безопасности. 256-разрядная подпись ECDSA обладает такой же степенью защиты, как и 3072-разрядная подпись RSA [9].

*Алгоритм ECDH*

Протокол Диффи-Хеллмана на эллиптических кривых – ECDH (Elliptic curve Diffie–Hellman) – криптографический протокол, позволяющий двум сторонам, имеющим пары ключей, получить общий секретный ключ, используя незащищённый от прослушивания канал связи [10].

Алгоритм Диффи Хеллмана на эллиптических кривых (ECDH) отличается от общего алгоритма Диффи Хеллмана (DH) тем, что он основан на задаче дискретного логарифмирования эллиптической кривой (ECDLP) вместо задачи дискретного логарифмирования (DLP). Это означает, что мы можем обойтись ключами меньшей длина, чем при использовании DH.

*Опишем общий алгоритм ECDH:*

– Выбор эллиптической кривой $E(a,b)$ и базовой точки $P$ (генератора кривой).

– Пользователь **A** выбирает свой секретный ключ $K_A$ ($K_A \in [2, n-1]$), определяет открытый ключ $Q_A = K_A \cdot P$ и отправляет пользователю **B** свой открытый ключ $Q_A$.

– Пользователь **B** получает ключ открытый $Q_A$, выбирает секретный ключ $K_B$, определяет свой открытый ключ $Q_B = K_B \cdot P$ и отправляет пользователю **A** свой открытый ключ $Q_B$.

– Пользователь **A** вычисляет общий секретный ключ $X_K = K_A \cdot Q_B = K_A \cdot K_B \cdot P$.

– Пользователь **B** вычисляет общий секретный ключ $X_K = K_B \cdot Q_A = K_B \cdot K_A \cdot P$.

При использовании алгоритма ECDH обеим сторонам необходимо выбрать общую эллиптическую кривую $E(a,b)$. $Q_A$ и $Q_B$ являются открытыми ключами IoT-устройства и сервера соответственно, $K_A$ и $K_B$ являются закрытыми ключами. Устройство IoT и сервер умножают базовую точку $P$ на свои закрытые ключи. В результате получаются точки на эллиптической кривой – открытые ключи.

Общий секретный ключ – это координата x результирующей точки, которую они получают после умножения своих соответствующих закрытых ключей на открытый ключ друг друга [11].

*Выбор эллиптической кривой для ECDH*

После обмена ключами полученный общий секретный ключ можно использовать для алгоритма симметричного шифрования. В качестве такого алгоритма можно использовать, например, AES-128 (Advanced Encryption Standard с 128-битным секретным ключом). Степень защиты алгоритма обмена ключами (ECDH) не должна уступать степени защиты используемого алгоритма традиционного шифрования (AES-128).

Для обеспечения сопоставимого уровня защиты AES-128 можно использовать алгоритм Диффи-Хеллмана на эллиптических кривых с диной ключа 256-283 бит.

Будем использовать эллиптическую кривую Curve25519, с помощью которой генерируются 256 битные ключи. Кривая имеет параметры [12]:

$p$ = 0x7fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffed

$a$ = 0x76d06

$b$ = 0x01

$P$ = (0x09, 0x20ae19a1b8a086b4e01edd2c7748d14c923d4d7e6d7c61b229e9c5a27eced3d9)

$n$ = 0x1000000000000000000000000000000014def9dea2f79cd65812631a5cf5d3ed

$h$ = 8

Метод обмена ключами при помощи выполнения операций над эллиптической кривой Curve25519 носит название X25519. Сам алгоритм обмена ключами аналогичен ECDH [13]:

– Пользователь **А** генерирует $a$ - 32-битное случайное число, вычисляет $K_A$ = X25519($a$, 9) и передает пользователю **Б**, где 9 – это $x$-координата базовой точки.

– **Б** генерирует $b$ - 32-битное случайное число, вычисляет = X25519($b$, 9) и передает **А**.

– Используя сгенерированные значения и полученные входные данные, **А** вычисляет X25519($a$, $K_B$), а **Б** вычисляет X25519($b$, $K_A$).

– Теперь оба пользователя могут использовать

$K$ = X25519($a$, X25519($b$, 9)) = X25519($b$, X25519($a$, 9)) в качестве общего секрета.

*Пример использования X25519:*

Секретный ключ **А**:

$a$ = 0x77076d0a7318a57d3c16c17251b26645df4c2f87ebc0992ab177fba51db92c2a

Открытый ключ **А**:

$K_A$ = 0x8520f0098930a754748b7ddcb43ef75a0dbf3a0d26381af4eba4a98eaa9b4e6a

Секретный ключ **Б**:

$b$ = 0x5dab087e624a8a4b79e17f8b83800ee66f3bb1292618b6fd1c2f8b27ff88e0eb

Открытый ключ **Б**:

$K_B$ = de9edb7d7b7dc1b4d35b61c2ece435373f8343c85b78674dadfc7e146f882b4f

Секретный ключ, полученный обеими сторонами после обмена:

$K$ = 4a5d9d5ba4ce2de1728e3bf480350f25e07e21c947d19e3376f09b3c1e161742

В результате обмена оба пользователя получили общий секретный ключ $K$.

*Заключение*

Поскольку асимметричная криптография основана на сложности решения задачи дискретного логарифма, то криптосистемы с открытым ключом безопасны благодаря тому, что вызывает сложность разложение составного числа на простые множители. При использовании алгоритмов на эллиптических кривых предполагается, что не существует субэкспоненциальных алгоритмов для решения задачи дискретного логарифмирования в группах их точек. При этом сложность задачи определяется порядком группы точек эллиптической кривой. И, следовательно, для достижения того же уровня безопасности, как и в RSA необходимы группы меньших порядков, что неизбежно приводит к уменьшению затрат на хранение и передачу информации. В данной работе были рассмотрены основы криптографии на эллиптических кривых, преимущества использования ECDLP алгоритмов для IoT устройств. Был кратко рассмотрен алгоритм цифровой подписи ECDSA и более глубоко был изучен алгоритм обмена ключами ECDH, для которого выбрана кривая Curve25519 и метод обмена ключами X25519. Данный алгоритм обеспечивает 128-битный уровень защиты, что соответствует уровню симметричного шифрования AES-128, который может использоваться после обмена ключами. Основное преимущество криптографии на эллиптических кривых – это малый размер ключа по сравнению с другими схемами асимметричного шифрования. Это свойство особенно важно при реализации криптографических протоколов в условиях ограниченности ресурсов памяти и производительности, например, при программировании смарт-карт. Но также понятно, что при постоянно улучшающейся производительности компьютеров данные шифры становиться более уязвимыми при малой длине ключа. А при увеличении длины ключа схемы, основанные на эллиптических кривых, приобретают еще большее преимущество над другими схемами.

## Литература


1. State of IoT 2023: Number of connected IoT devices. [Электронный ресурс]: https://iot-analytics.com/number-connected-iot-devices/

2. Калхиташвили Д. Ш. Операционные системы интернета вещей: возможности, проблемы и решения / Д. Ш. Калхиташвили — Москва: РАНХиГС, 2023. — 5 с.

3. Рябко, Б. Я. Криптографические методы защиты информации: учеб. пособие / Б. Я. Рябко, А. Н. Фионов. — 2-е изд., стер. — М.: Горячая линия – Телеком, 2012. — 229 с.

4. NIST Special Publication 800-57 Part 3 Revision 1. Recommendation for Key Management. Part 3: Application-Specific Key Management Guidance. / NIST – 2015 – P. 52.

5. NIST Special Publication 800-57 Part 1 Revision 5 Recommendation for Key Management: Part 1 – General. / NIST – 2020 – P. 54 – 55.

6. Жданов, О. Н. Применение эллиптических кривых в криптографии: учеб. пособие / О. Н. Жданов, Т. А. Чалкин. — Красноярск: СибГАУ, 2011 - 65 с.

7. Национальный стандарт Российской Федерации. Криптографическая защита информации. [Электронный ресурс]: https://www.altell.ru/legislation/standards/gost-34.10-2012.pdf

8. Chandrasekhara, K.R. Elliptic Curve based authenticated session Key establishment protocol for High Security Applications in Constrained Network environment / K.R. Chandrasekhara, M.P. Pillai1 and Sebastian, 2010. [Электронный ресурс]: http://www.arxiv.org/pdf/1202.1895

9. ECDSA: Elliptic Curve Signatures. [Электронный ресурс]: https://cryptobook.nakov.com/digital-signatures/ecdsa-sign-verify-messages (дата обращения: 12.04.2024)

10. Fatma Ahmed, Dalia Elkamchouchi. A New Efficient Protocol for Authenticated Key Agreement // International Journal of Computer and Communication Engineering – 2013 – Vol. 2, No. 4. – P. 1 – 3.

11. Rakel Haakegaard, Joanna Lang. The Elliptic Curve Diffie-Hellman (ECDH) / 2015 – P. 1 – 2.

12. Standard curve database. Curve25519. [Электронный ресурс]: https://neuromancer.sk/std/other/Curve25519 (дата обращения: 19.04.2024)

13. RFC 7748. Elliptic Curves for Security. / IRTF – 2016 – P. 14.


## References


1. State of IoT 2023: Number of connected IoT devices. [Электронный ресурс]: https://iot-analytics.com/number-connected-iot-devices/

2. Kalhitashvili D. Sh. Operacionnye sistemy interneta veshhej: vozmozhnosti, problemy i reshenija / D. Sh. Kalhitashvili — Moskva: RANHiGS, 2023. — 5 s.

3. Rjabko, B. Ja. Kriptograficheskie metody zashhity informacii: ucheb. posobie / B. Ja. Rjabko, A. N. Fionov. — 2-e izd., ster. — M.: Gorjachaja linija – Telekom, 2012. — 229 s.

4. NIST Special Publication 800-57 Part 3 Revision 1. Recommendation for Key Management. Part 3: Application-Specific Key Management Guidance. / NIST – 2015 – P. 52.

5. NIST Special Publication 800-57 Part 1 Revision 5 Recommendation for Key Management: Part 1 – General. / NIST – 2020 – P. 54 – 55.

6. Zhdanov, O. N. Primenenie jellipticheskih krivyh v kriptografii: ucheb. posobie / O. N. Zhdanov, T. A. Chalkin. — Krasnojarsk: SibGAU, 2011 - 65 s.

7. Nacional'nyj standart Rossijskoj Federacii. Kriptograficheskaja zashhita informacii. [Jelektronnyj resurs]: https://www.altell.ru/legislation/standards/gost-34.10-2012.pdf

8. Chandrasekhara, K.R. Elliptic Curve based authenticated session Key establishment protocol for High Security Applications in Constrained Network environment / K.R. Chandrasekhara, M.P. Pillai1 and Sebastian, 2010. [Электронный ресурс]: http://www.arxiv.org/pdf/1202.1895

9. ECDSA: Elliptic Curve Signatures. [Электронный ресурс]: https://cryptobook.nakov.com/digital-signatures/ecdsa-sign-verify-messages (дата обращения: 12.04.2024)

10. Fatma Ahmed, Dalia Elkamchouchi. A New Efficient Protocol for Authenticated Key Agreement // International Journal of Computer and Communication Engineering – 2013 – Vol. 2, No. 4. – P. 1 – 3.

11. Rakel Haakegaard, Joanna Lang. The Elliptic Curve Diffie-Hellman (ECDH) / 2015 – P. 1 – 2.

12. Standard curve database. Curve25519. [Электронный ресурс]: https://neuromancer.sk/std/other/Curve25519 (дата обращения: 19.04.2024)

13. RFC 7748. Elliptic Curves for Security. / IRTF – 2016 – P. 14.

**ВОРОБЬЕВ Артем Павлович,** студент, кафедра Технология твердых химических веществ Казанского национального исследовательского технологического университета. 420015, Республика Татарстан, г. Казань, ул. Карла Маркса, 68. E-mail: drsleepwalker@yandex.ru

**КРОТОВА Елена Львовна,** кандидат физико-математических наук, доцент, кафедра Высшей математики, Пермский национальный исследовательский политехнический университет. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: lenkakrotova@yandex.ru

**ВОРОБЬЕВА Елена Юрьевна,** старший преподаватель, кафедра Прикладной математики, Пермский национальный исследовательский политехнический университет. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: lena-vorobey@yandex.ru

**VOROBEV Artem Pavlovich,** student, Department of Solid Chemical Substances Technology, Kazan National Research Technological University. 420015, Republic of Tatarstan, Kazan, Karl Marx St., 68. Email: drsleepwalker@yandex.ru

**KROTOVA Elena Lvovna,** Candidate of Physical and Mathematical Sciences, Associate Professor, Department of Higher Mathematics, Perm National Research Polytechnic University. 614990, Perm Krai, Perm, Komsomolsky Prospekt, 29. Email: lenkakrotova@yandex.ru

**VOROBEVA Elena Yuryevna,** Senior Lecturer, Department of Applied Mathematics, Perm National Research Polytechnic University. 614990, Perm Krai, Perm, Komsomolsky Prospekt, 29. Email: lena-vorobey@yandex.ru

УДК 004.93 Вестник УрФО № 3(53) / 2024, с. 32–43

**Котенко В. В., Румянцев К. Е., Хаджиева Л. К.** DOI: 10.14529/secur240304

# *ПАРАМЕТРЫ НЕЙРОЛИНГВИСТИЧЕСКОЙ ИДЕНТИФИКАЦИИ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА*

*Исследована возможность нейролингвистической текстовой идентификации систем искусственного интеллекта (ИИ). Для постановки задачи на четырех языках использованы системы ИИ (второго, третьего и четвертого поколений). В исследовании применён программный комплекс оценки информационных параметров нейролингвистической текстовой идентификации. Результаты исследований подтверждают возможность применения в качестве параметров нейролингвистической идентификации информационных характеристик текстовой составляющей систем искусственного интеллекта. Приведены зависимости основных и производных параметров нейролингвистической текстовой идентификации от изменений систем искусственного интеллекта для результатов при постановке задачи на разных языках. Проведен анализ изменения показателей систем искусственного интеллекта по основным и производным параметрам, но для поставленной задачи на четырех языках одной СИИ, а также для разных СИИ. По результатам анализа установлено, что значения основных и производных параметров нейролингвистической текстовой идентификации систем искусственного интеллекта при постановке одной и той же задачи на разных языках одной системе ИИ отличаются при переходе от одного языка на другой в одной системе ИИ, при переходе от одной системы ИИ к другой, при переходе от одной системы к другой с сохранением одного и того же языке. Исследование подтверждает возможность использовать в качестве параметров нейролингвистической текстовой идентификации систем искусственного интеллекта информационные характеристики текстовой составляющей.*

***Ключевые слова:*** *нейролингвистическая идентификация, искусственный интеллект, избыточность, зависимость параметров, информационная емкость.*

# *PARAMETERS OF NEURO-LINGUISTIC IDENTIFICATION OF ARTIFICIAL INTELLIGENCE SYSTEMS*

*The possibility of neuro-linguistic textual identification of artificial intelligence (AI) systems is investigated. AI systems (second, third and fourth generations) were used to formulate the problem in four languages. The study uses a software package for evaluating the information parameters of neuro-linguistic textual identification. The research results confirm the possibility of using the information characteristics of the text component of artificial intelligence systems as parameters of neuro-linguistic identification. The dependences of the main and derived parameters of neuro-linguistic textual identification on changes in artificial intelligence systems for the results when setting the problem in different languages are presented. The analysis of changes in the indicators of artificial intelligence systems by basic and derived parameters, but for the task in four languages of the same SII, as well as for different SII, is carried out. Based on the results of the analysis, it was found that the values of the basic and derived parameters of the neuro-linguistic textual identification of artificial intelligence systems when setting the same task in different languages of one AI system differ when switching from one language to another in one AI system, when switching from one AI system to another, when switching from one system to another with keeping the same language. The study confirms the possibility of using the information characteristics of the text component as parameters of the neuro-linguistic textual identification of artificial intelligence systems.*

***Keywords:*** *neurolinguistic identification, artificial intelligence, redundancy, parameter dependence, information capacity.*

**Введение**

Определение способов, по которым будет возможно выявлять, применялись ли системы искусственного интеллекта (СИИ) в решении задач в разных сферах и направлениях деятельности человека или задачи решались самим человеком (интеллектуальной системой) в настоящее время является одной из основных задач современности, так как системы искусственного интеллекта способны принести как пользу так и колоссальный вред в зависимости от того кто является его пользователем, так как системы искусственного интеллекта могут хранить или обрабатывать информацию. Последнее определяет важность решения проблем идентификации и обнаружения систем искусственного интеллекта (СИИ).

Нейролингвистическая идентификация является новым подходом в оправлении применения как систем искусственного интеллекта, так и интеллектуальных систем по параметрам идентификатора.

Исследования, проведённые ранее авторами, показали, что значения основных и производных параметров нейролингвистической текстовой идентификации систем искусственного интеллекта при постановке одной и той же задачи разным системам искусственного интеллекта значительно отличаются. а информационные характеристики текстовой составляющей систем искусственного интеллекта можно использовать в качестве параметров нейролингвистической текстовой идентификации систем искусственного интеллекта [1].

В качестве параметров идентификатора выступают: коэффициент избыточности, коэффициент вербальности, эмпирическая энтропия, информационная емкость.

Проведённые авторами ранее исследования показали результативность данного подхода при как при идентификации интеллектуальных систем (людей) так и при идентификации систем искусственного интеллекта.

При исследовании использовались тексты по одинаковой тематике, произвольно формируемой различными интеллектуальными системами. Применение предложенной нейролингвистической текстовой идентификации показало возможность довольно точной идентификации интеллектуальных систем.

В настоящем исследовании решается проблема применения данного подхода к идентификации систем искусственного интеллекта: во-первых, при постановке одной задачи на разных языках одной системе, во-вторых, при постановке одной задачи на разных языках разным системам искусственного интеллекта, в-третьих, определение изменения параметров при переходе от одной системы искусственного интеллекта к другой. По итогам исследования можно будет определить состояния основных и производных параметров в разных нестандартных ситуациях и определить вероятность применения параметров в качестве идентификатора как интеллектуальных систем, так и систем искусственного интеллекта.

**Постановка задачи**

Ставилась задача выявления фактора изменения параметров нейролингвистической текстовой идентификации при постановке одной и той же задачи на разных языках системам искусственного интеллекта разных поколений. Успешное решение этой задачи позволяло показать индивидуальность систем искусственного интеллекта и их способность генерировать одну и ту же задачу на разных языках [15-20].

Целью исследования является анализ нейролингвистической текстовой идентификации систем искусственного интеллекта на разных языках и выявления вероятности использования параметров в качестве факторов нейролингвистической идентификации систем искусственного интеллекта.

Задачами исследования являются:

1. Количественная оценка отличий значений основных и производных параметров нейролингвистической текстовой идентификации систем искусственного интеллекта при постановке одной и той же задачи на трех языках одной системе ИИ, при постановке одной и той же задачи на четырех языках разным системам ИИ.

2. Анализ основных и производных параметров нейролингвистической текстовой идентификации систем искусственного интеллекта.

**Описание исследований**

В исследовании проведен анализ параметров систем искусственного интеллекта: GigaChat(2), YandexGPT(3), Gerwin (3), Gemini(3), RuGPT3 (3), CopyMonkey (3), Copilot(4), ChatGPT (4), Bing(4), , TurboText (4) , для которых приняты сокращения СИИ-1, СИИ-2, …, СИИ-n. Всем исследуемым системам искусственного интеллекта определена одна и та же задача для решения. Постановка задачи формулируется на четырех языках русском, английском, немецком и французиком языке. Объём выдаваемого каждой системой искусственного интеллекта результата одинаковый для всех запросов [1]. Задачей исследования было выявление фактора изменения параметров нейролингвистической текстовой идентификации при постановке одной и той же задачи на разных языках системам искусственного интеллекта разных поколений. При постановке одной и той же задачи на четырех языках преимущественно русском, английском, немецком и французиком параметры разных систем ИИ предположительно должны были иметь относительно незначительные изменения результатов. Однако, исследование показывает, что результат одной задачи на разных языках каждой системы ИИ индивидуален отличается от остальных [2, 3]. Показатели всех параметров меняются: во-первых, при обработке в одной системе ИИ одной задачи на разных языках, во-вторых, при переходе от одной системы ИИ к другой при постановке задачи на одном языке, в-третьих, при переходе от одной системы ИИ к другой при постановке задачи на разных зыках [5 - 10].

Программный комплекс при обработке данных разных СИИ как на одном, так и на разных языках выдает результаты основных показателей: информационной емкости, энтропии и избыточности.

Информационная емкость ансамбля дискретного источника определяется из числа элементов выборочного пространства $K$ по формуле:

$$H_{max}[U] = log_2 K; \quad (1)$$

Эмпирическая энтропия определяется в виде:

$$H_L(U) = M\left[J^*[u_i]\right], \quad (2)$$

где $J^*[u_i]$ оценка количества информации в сообщении $u_i$.

В общем виде избыточность дискретных источников информации определяется как:

$$B[U] = H_{max}[U] - H[U], \tag{3}$$

где $H_{max}[U]$ – максимально возможная энтропия выборочного пространства ансамбля U источника; $H[U]$ – энтропия источника.

Для расчёта производных параметров коэффициента избыточности $\mu_B$ и коэффициента вербальности $G_B$ использованы формулы:

$$\mu_B = \frac{H_{Bmax} - H_B}{H_{Bmax}}; \tag{4}$$

$$G_B = \frac{H_B}{H_{Bmax} - H_B}, \tag{5}$$

где $H_{Bmax}$ - среднее значение информационной емкости;

$H_B$ - среднее значение энтропии.

Коэффициент избыточности показывает, какая доля возможной информационной емкости на букву алфавита не используется алфавитом. Так как является безразмерной величиной, то его обычно измеряют в процентах [14 - 17].

Сводка дискретных алгоритмов фильтрации:

Модель сообщения:

$$\boldsymbol{J_x}(j+1) = \boldsymbol{\Phi}(j+1, j)\boldsymbol{J}_x(j) + \boldsymbol{\Gamma}(j)\boldsymbol{J}_w(j). \tag{6}$$

Модель наблюдения:

$$\boldsymbol{J}_z(j) = \boldsymbol{H}(j)\boldsymbol{J_x}(j) + \boldsymbol{J}_v(j). \tag{7}$$

Априорные данные:

$$\mathrm{E}\{\boldsymbol{J_w}(\boldsymbol{j})\} = 0; \mathrm{E}\{\boldsymbol{J_v}(j)\} = 0; \mathrm{E}\{\boldsymbol{J_x}(0)\} = \mu_{\boldsymbol{x}}(0);$$

$$cov\{\boldsymbol{J_w}(j), \boldsymbol{J_w}(k)\} = \boldsymbol{V}_{\boldsymbol{J_w}}(j)\delta_K(j-k);$$

$$cov\{\boldsymbol{J_v}(j), \boldsymbol{J_v}(k)\} = \boldsymbol{V}_{\boldsymbol{J_v}}(j)\delta_K(j-k);$$

$$cov\{\boldsymbol{J_w}(j), \boldsymbol{J_v}(k)\} = cov\{\boldsymbol{J_x}(0), \boldsymbol{J_v}(k)\} = cov\{\boldsymbol{J_x}(0), \boldsymbol{J_w}(k)\} = 0;$$

$$var\{\boldsymbol{J_x}(0)\} = \boldsymbol{V}_{\widetilde{\boldsymbol{J_x}}}.$$

Алгоритм фильтрации:

$$\boldsymbol{J}_{\boldsymbol{x}}^{*}(j) = \Phi(j, j-1)\boldsymbol{J}_{\boldsymbol{x}}^{*}(j-1) + \boldsymbol{K}(j)\left[\boldsymbol{J_z}(j) - \boldsymbol{H}_{\boldsymbol{J_x}}(j)\Phi(j, j-1)\boldsymbol{J}_{\boldsymbol{x}}^{*}(j-1)\right]. \tag{8}$$

Вычисление коэффициента усиления:

$$\boldsymbol{K}(j) = \boldsymbol{V}_{\widetilde{\boldsymbol{J_x}}}(j|j-1)\boldsymbol{H}^T(j)\left[\boldsymbol{H}(j)\boldsymbol{V}_{\widetilde{\boldsymbol{J_x}}}(j|j-1)\boldsymbol{H}^T(j) + \boldsymbol{V}_{\boldsymbol{J_v}}(j)\right]^{-1} = \boldsymbol{V}_{\widetilde{\boldsymbol{J_x}}}(j)\boldsymbol{H}^T(j)\boldsymbol{V}_{\boldsymbol{J_v}}{}^{-1}(j) \tag{9}$$

Величина априорной дисперсии:

$$\boldsymbol{V}_{\widetilde{\boldsymbol{J_x}}}(j+1|j) = \Phi(\boldsymbol{j}+\boldsymbol{1}, j)\boldsymbol{V}_{\widetilde{\boldsymbol{J_x}}}(j)\Phi^T(\boldsymbol{j}+1, j) + \boldsymbol{\Gamma}(j)\boldsymbol{V}_{\boldsymbol{J_w}}(j)\boldsymbol{\Gamma}^T(j). \tag{10}$$

Уравнение для апостериорной дисперсии:

$$\boldsymbol{V}_{\widetilde{J_x}}(j) = [\boldsymbol{I}_{\boldsymbol{x}} - \boldsymbol{K}(j)\boldsymbol{H}(j)]\boldsymbol{V}_{\widetilde{J_x}}(j \mid j-1). \quad (11)$$

Начальные условия:

$$\boldsymbol{J}_{\boldsymbol{x}}^{*}(0 \mid 0) = \boldsymbol{J}_{\boldsymbol{x}}^{*}(0) = \mu_{J_x}(0), \boldsymbol{V}_{\widetilde{J_x}}(0|0) = \boldsymbol{V}_{\widetilde{J_x}}(0) = \boldsymbol{V}_{J_x}(0) \quad (0)$$

Анализ структурой схемы рис. 1 показывает, что в фильтре реализуется идея предсказания – коррекции. Предыдущая оценка $\boldsymbol{J}_{\boldsymbol{x}}^{*}(j-1)$ экстраполируется на один шаг вперед и затем используется для получения наилучшей оценки нового наблюдения $\boldsymbol{J}_{\boldsymbol{z}}(j)$ основанной на всех предыдущих наблюдениях [1]. Ошибка между «наилучшей оценкой» текущего наблюдения и фактическим наблюдением, а именно $\mathcal{Y}(j|j-1)$ или $\widetilde{\boldsymbol{J}_{\boldsymbol{z}}}(j \mid j-1)$, представляет собой новую информацию [компоненту $\boldsymbol{J}_{\boldsymbol{z}}(j)$, ортогональную $\boldsymbol{J}_{\boldsymbol{z}}(j-1)$].

Ошибка взвешивается с весом $\boldsymbol{K}(j)$, учитывающим значение дисперсий входного процесса, измерения и ошибки оценивания для формирования сигнала коррекции. Сигнал коррекции складывается с предсказанной оценкой и в результате получается новая оценка [2].

*Таблица 1*

**Параметры нейролингвистической текстовой идентификации систем искусственного интеллекта**

| Системы искусственного интеллекта | Информационная емкость $H_{Bmax}$ | | | | Энтропия $H_B$ | | | | Избыточность $B$ | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Р | А | Н | Ф | Р | А | Н | Ф | Р | А | Н | Ф |
| СИИ-1 (GigaChat 2) | 4,45 | 4,85 | 3,97 | 4,03 | 1,73 | 1,65 | 1,55 | 1,53 | 2,72 | 3,20 | 2,42 | 2,48 |
| СИИ-2 (YandexGPT 3) | 5,93 | 6,34 | 6,54 | 5, 28 | 1,79 | 1,59 | 1,65 | 1,78 | 4,14 | 4,75 | 4,89 | 3,57 |
| СИИ-3 (Gerwin 3) | 6,11 | 6,42 | 6,48 | 5,10 | 1,85 | 1,74 | 1,77 | 1,62 | 4,26 | 4,68 | 4,71 | 3,48 |
| СИИ-4 (Gemini 3) | 5,28 | 6,54 | 6,65 | 5,35 | 1,70 | 1,67 | 1,74 | 1,53 | 3,58 | 4,87 | 4,91 | 3,82 |
| СИИ-5 (RuGPT 3) | 5,45 | 5,66 | 5,71 | 4,46 | 1,74 | 1,72 | 1,81 | 1,54 | 3,71 | 3,94 | 3,90 | 2,92 |
| СИИ-6 (CopyMonkey 3) | 5,69 | 5,33 | 5,53 | 4,85 | 1,93 | 1,71 | 1,88 | 1,56 | 3,76 | 3,62 | 3,65 | 3,29 |
| СИИ-7 (Copilot 4) | 4,93 | 4,94 | 5,34 | 5,23 | 1,65 | 1,77 | 1,82 | 1,76 | 3,20 | 3,17 | 3,52 | 3,47 |
| СИИ-8 (ChatGPT 4) | 4,81 | 5,43 | 4,67 | 5,48 | 1,69 | 1,86 | 1,75 | 1,98 | 3,12 | 3,57 | 2,92 | 3,50 |
| СИИ-9 (Bing 4) | 4,48 | 5,78 | 5,10 | 5,24 | 1,78 | 1,63 | 1,93 | 1,88 | 2,85 | 4,03 | 3,17 | 3,36 |
| СИИ-10 (TurboText 4) | 5,43 | 5,65 | 5,28 | 5,78 | 1,94 | 1,81 | 1,84 | 1,94 | 3,49 | 3,84 | 3,44 | 3,84 |

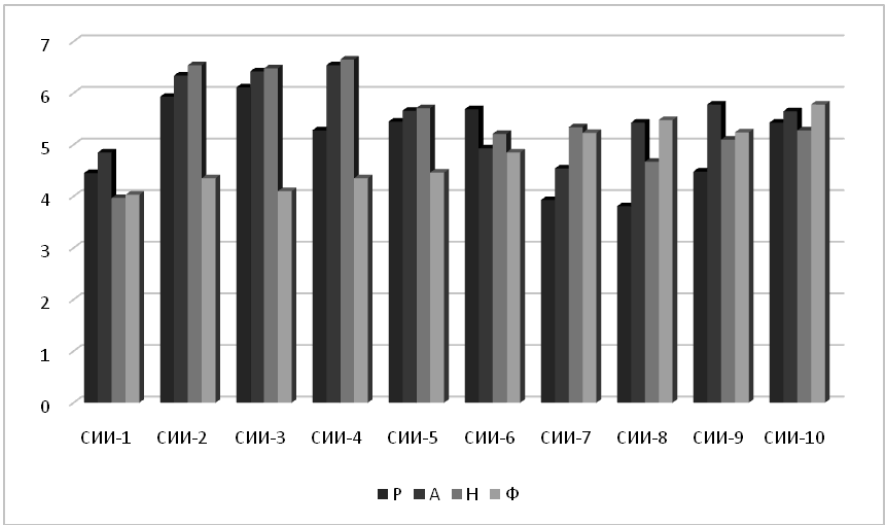


Рис. 1. Информационная емкость нейролингвистической текстовой информации систем ИИ

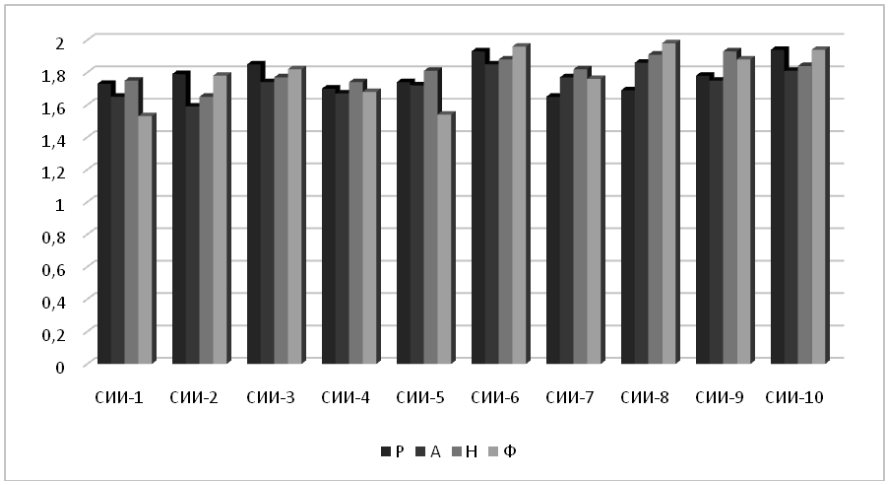


Рис. 2. Энтропия нейролингвистической текстовой информации систем ИИ

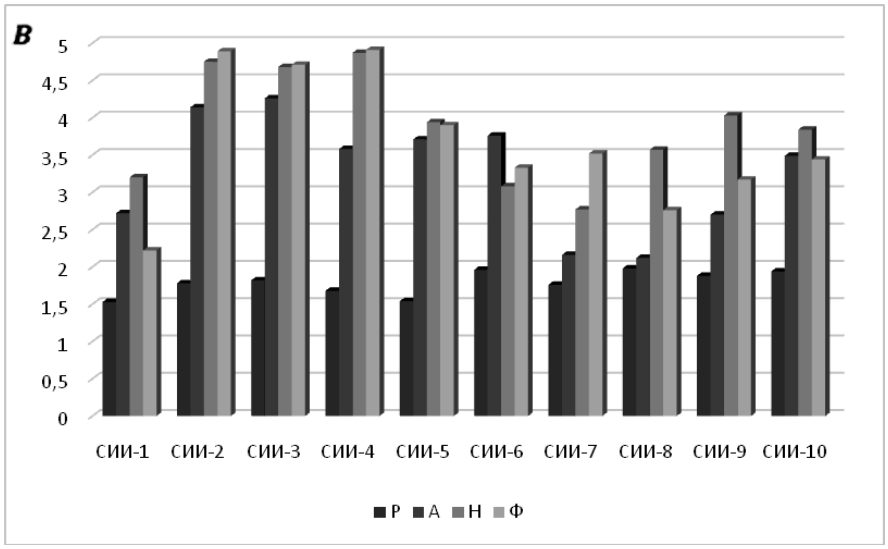


Рис. 3. Избыточность нейролингвистической текстовой информации систем ИИ

Результаты основных и производных параметров приведены в таблицах 1 и 3. Результаты средних значений основных и производных параметров сведены в таблицы 2 и 4.

**Результаты исследований**

Проведем анализ параметров, полученных в десяти системах искусственного интеллекта разных поколений как российского, так и иностранного производства на четырех языках (русском, английском, немецком и французском). Результаты полученных материалов были переведены в необходимый формат и проверены с помощью апробированного программного комплекса оценки информационных параметров нейролингвистической текстовой идентификации интеллектуальных систем [2].

Исследовано десять систем искусственного интеллекта разных поколений, которые разработаны как российскими, так и иностранными разработчиками, постанова задачи формулировалась на четырех языках (русском, английском, немецком и французском). Результаты оценки основных параметров нейролингвистической текстовой идентификации систем искусственного интеллекта на разных языках сведены в таблицу 1.

Результаты исследования зависимости основных параметров нейролингвистической текстовой идентификации систем ИИ на разных языках приведены на рисунках 1, 2 и 3.

Полученные результаты показывают, что минимальное значение информационной емкости текста систем искусственного интеллекта соответствует: Р - СИИ-8 – $H_{Bmax}$= 3,81; А - СИИ-7 – $H_{Bmax}$= 4,54; Н - СИИ-1 – $H_{Bmax}$= 3,97; Ф - СИИ-1 – $H_{Bmax}$= 4,03. Максимальное значение информационной емкости текста систем искусственного интеллекта соответствует: Р - СИИ-2 – $H_{Bmax}$= 5,93; А - СИИ-4 – $H_{Bmax}$= 6,54; Н - СИИ-4 – $H_{Bmax}$= 6, 65; Ф - СИИ-10 – $H_{Bmax}$= 5,78. Среднее значение информационной емкости: Р – $\dot{H}_{Bmax}$= 4,87; А – $\dot{H}_{Bmax}$= 5,54; Н – $\dot{H}_{Bmax}$= 5,31; Ф – $\dot{H}_{Bmax}$= 4,90. Минимальное значение энтропии текста систем искусственного интеллекта соответствует: Р – СИИ-7 – $H_B$= 1,65; А – СИИ-1 – $H_B$= 1,65; Н – СИИ-2 – $H_B$= 1,65; Ф – СИИ-1 – $H_B$= 1,53. Максимальное значение энтропии текста систем искусственного интеллекта соответствует: Р – СИИ-10 – $H_B$= 1,94; А – СИИ-8 – $H_B$= 1,86; Н – СИИ-8 – $H_B$= 1,93; Ф – СИИ-8 – $H_B$= 1,98. Среднее значение энтропии: Р – $H_B$= 1,79; А – H_B= 1,75; Н – $H_B$= 1,79; Ф – $H_B$= 1,75. Минимальное значение избыточности текста систем искусственного интеллекта соответствует: Р – СИИ-8 – B= 2,12; А – СИИ-7 – B= 2,77; Н – СИИ-1 – B= 2,22; Ф – СИИ-3 – B= 2,28;. Максимальное значение избыточности текста систем искусственного интеллекта соответствует: Р – СИИ-3 – B= 4,26; А – СИИ-4 – B= 4,87; Н – СИИ-4 – B= 4,91; Ф – СИИ-10 – B= 3,84. Среднее значение виртуальной избыточности Р – B= 4,25; А – B= 3,82; Н – B= 3,56; Ф – B= 4,20.

Средние значения основных параметров нейролингвистических текстовых идентификаторов систем искусственного интеллекта сведены в таблицу 2.

В таблицу 3 сведены результаты расчётов производных параметров нейролингвистической текстовой идентификации систем искусственного интеллекта: коэффициент избыточности и коэффициент вербальности.

Результаты исследования зависимости производных параметров нейролингвистической текстовой идентификации систем искусственного интеллекта приведены на рисунках 4 и 5.

Установлено, что минимальное значение коэффициента избыточности текста систем искусственного интеллекта соответствует: Р - СИИ-7 – $\mu_B$= 0,549; А - СИИ-6 – $\mu_B$= 0,724; Н - СИИ-1 – $\mu_B$= 0,559; Ф - СИИ-3 – $\mu_B$= 0,556. Максимальное значение коэффициента избыточности текста систем искусственного интел-

*Таблица 2*

**Среднее значение параметров нейролингвистических текстовых идентификаторов систем искусственного интеллекта**

| **Среднее значение информационной емкости $H_{Bmax}$** | | | | **Среднее значение энтропии $H_B$** | | | | **Среднее значение избыточности *B*** | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Р** | **А** | **Н** | **Ф** | **Р** | **А** | **Н** | **Ф** | **Р** | **А** | **Н** | **Ф** |
| 4,87 | 5,54 | 5,31 | 4,9 | 1,79 | 1,75 | 1,79 | 1,75 | 4,25 | 3,82 | 3,56 | 4,2 |

*Таблица 3*

**Производные параметры систем искусственного интеллекта**

| СИИ | Коэффициент избыточности, $\mu_B$ | | | | Коэффициент вербальности, $G_B$ | | | |
|---|---|---|---|---|---|---|---|---|
| | Р | А | Н | Ф | Р | А | Н | Ф |
| СИИ-1 (GigaChat 2) | 0,611 | 0,659 | 0,559 | 0,615 | 0,636 | 0,515 | 0,64 | 0,616 |
| СИИ-2 (YandexGPT 3) | 0,698 | 0,749 | 0,747 | 0,59 | 0,434 | 0,334 | 0,337 | 0,498 |
| СИИ-3 (Gerwin 3) | 0,697 | 0,728 | 0,726 | 0,556 | 0,432 | 0,371 | 0,375 | 0,465 |
| СИИ-4 (Gemini 3) | 0,678 | 0,744 | 0,738 | 0,613 | 0,474 | 0,342 | 0,354 | 0,401 |
| СИИ-5 (RuGPT 3) | 0,68 | 0,696 | 0,639 | 0,654 | 0,469 | 0,438 | 0,464 | 0,527 |
| СИИ-6 (CopyMonkey 3) | 0,66 | 0,624 | 0,583 | 0,595 | 0,513 | 0,472 | 0,515 | 0,474 |
| СИИ-7 (Copilot 4) | 0,549 | 0,61 | 0,659 | 0,663 | 0,503 | 0,538 | 0,517 | 0,507 |
| СИИ-8 (ChatGPT 4) | 0,556 | 0,657 | 0,591 | 0,669 | 0,541 | 0,521 | 0,599 | 0,565 |
| СИИ-9 (Bing 4) | 0,602 | 0,697 | 0,621 | 0,641 | 0,571 | 0,434 | 0,608 | 0,559 |
| СИИ-10 (TurboText 4) | 0,642 | 0,679 | 0,651 | 0,664 | 0,555 | 0,471 | 0,534 | 0,505 |

лекта соответствует: Р - СИИ-2 – $\mu_B$= 0,698; А - СИИ-2 – $\mu_B$= 0,749; Н - СИИ-2– $\mu_B$= 0,747; Ф - СИИ-8 – $\mu_B$= 0,669. Среднее значение коэффициента избыточности: Р – $\mu_B$= 0,898; А – $\mu_B$= 0,736; Н– $\mu_B$= 0,653; Ф – $\mu_B$= 0,612; Минимальное значение коэффициента вербальности текста систем искусственного интеллекта соответствует: Р - СИИ-2 – $G_B$= 0,432; А - СИИ-2 – $G_B$= 0,334; Н - СИИ-2 - $G_B$= 0,337; Ф – СИИ-4– $G_B$= 0,401. Максимальное значение коэффициента вербальности текста систем искусственного интеллекта соответствует Р - СИИ-1 – $G_B$= 0,634; А – СИИ-7 – $G_B$= 0,538; Н – СИИ-1 – $G_B$= 0,640; Ф – СИИ-1 – $G_B$= 0,616. Среднее значение коэффициента вербальности Р – $G_B$= 0,533; А – $G_B$= 0,436; Н – $G_B$= 0,488; Ф – $G_B$= 0,508.

Средние значения коэффициентов избыточности и вербальности систем искусственного интеллекта сведены в таблицу 4.

Исследования, проведённые авторами, показали, что проблема идентификации мозговых механизмов речевой деятельности может быть решена при использовании в качестве идентификатора количества информации, содержащегося в логических элементах речи (словах, слогах и т.п.).

В качестве параметров идентификатора в данном случае выступают: коэффициент избыточности, коэффициент вербальности, эм-

*Таблица 4*

**Среднее значение коэффициентов избыточности и вербальности систем искусственного интеллекта**

| Среднее значение коэффициента избыточности $\mu_B$ | | | | Среднее значение коэффициента вербальности $G_B$ | | | |
|---|---|---|---|---|---|---|---|
| Р | А | Н | Ф | Р | А | Н | Ф |
| 0,898 | 0,736 | 0,653 | 0,612 | 0,533 | 0,436 | 0,488 | 0,508 |

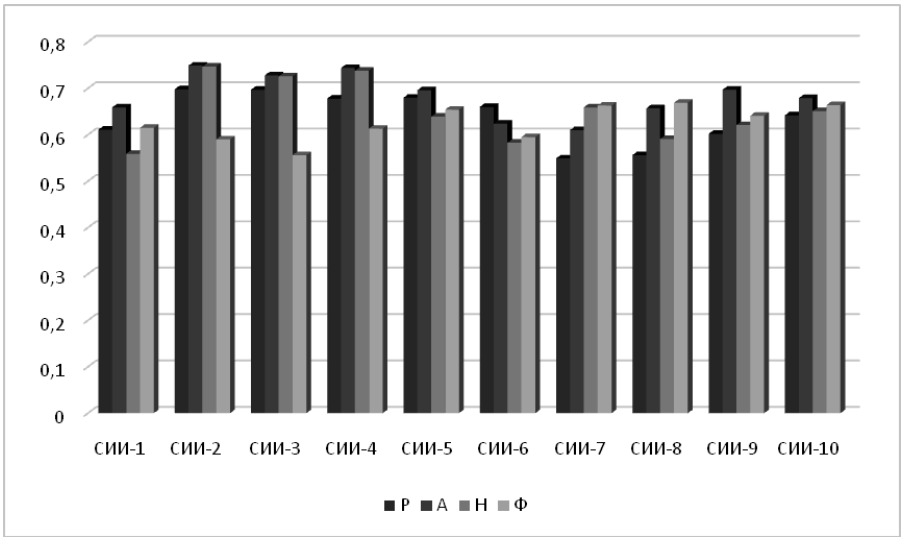


Рис. 4. Коэффициент избыточности нейролингвистической текстовой информации систем ИИ

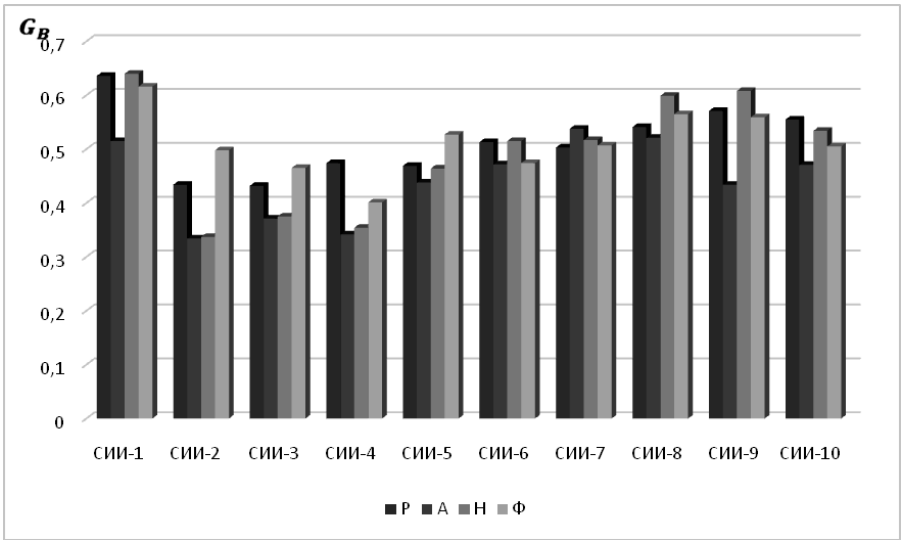


Рис. 5. Коэффициенты вербальности нейролингвистической текстовой информации систем ИИ

пирическая энтропия, информационная емкость. Все поставленные изначально задачи решены [6]. Определено, что значения основных и производных параметров нейролингвистической текстовой идентификации систем искусственного интеллекта при постановке одной и той же задачи разным системам ИИ значительно отличаются. Проанализированы основные и производные параметры нейролингвистической текстовой идентификации систем искусственного интеллекта [11-19]. Определены средние значения основных и производных параметров нейролингвистических текстовых идентификаторов систем искусственного интеллекта.

**Заключение**

Проведен анализ десяти систем искусственного интеллекта: одна система второго поколения, пять систем третьего поколения и четыре системы четвертого поколения. Всем системам ИИ определена одна и та же задача для решения на русском, английском, немецком и французском языках. Исследования подтверждают тот факт, что результат каждой СИИ индивидуален и отличается от всех остальных. Показатели параметров систем ИИ второго поколения отличаются от показателей параметров систем ИИ третьего поколения, показатели ИИ третьего поколения параметров отличаются от параметров си-

стем ИИ четвертого поколения. Изменения параметров наблюдаются как при переходе от одной системы ИИ к другой, так и при переходе от одного языка к другому.

Результаты исследований подтверждают доказанную в предыдущем исследовании возможность применения в качестве параметров нейролингвистической идентификации информационных характеристик текстовой составляющей систем искусственного интеллекта. Приведены зависимости основных и производных параметров нейролингвистической текстовой идентификации от изменений систем искусственного интеллекта для результатов при постановке задачи на четырех языках. Как и в предыдущем исследовании проведен анализ изменения показателей систем искусственного интеллекта по основным и производным параметрам, но для поставленной задачи на четырех языках одной СИИ, а также для разных СИИ. По результатам анализа установлено, что значения основных и производных параметров нейролингвистической текстовой идентификации систем искусственного интеллекта при постановке одной и той же задачи на разных языках одной системе ИИ отличаются при переходе от одного языка к другому в одной системе ИИ, при переходе от одной системы ИИ к другой на разных языках, при переходе от одной системы к другой с сохранением одного и того же языка. Исследование подтверждает возможность использовать в качестве параметров нейролингвистической текстовой идентификации систем искусственного интеллекта информационные характеристики текстовой составляющей.

**Литература**


1. Котенко В. В., Румянцев К. Е., Хаджиева Л. К. Оценка возможностей нейролингвистической идентификации систем искусственного интеллекта // Вестник УрФО. Безопасность в информационной сфере, Издательский центр ФГАОУ ВО «ЮУрГУ (НИУ)» № 2(52) / 2024 г. – С – 13-24.

2. Котенко В.В. Технологии информационного анализа пользовательского уровня телекоммуникационных систем. Учебное пособие // Ростов-на-Дону – Таганрог: Издательство Южного федерального университета, 2019. – 194 с

3. Котенко В.В., Румянцев К.Е. Теория информации. Учебное пособие // Ростов-на-Дону – Таганрог: Издательство Южного федерального университета, 2018. – 239 с.

4. Котенко В.В. Теория виртуализации и защита телекоммуникаций: монография – Таганрог: Изд-во ТТИ ЮФУ, 2011. – 236 с.

5. Котенко В.В. Румянцев К.Е., Котенко С.В. Методология идентификационного анализа инфокоммуникационных систем. Монография. – Ростов–на–Дону: Издательство Южного федерального университета, 2014. – 315 с.

6. Хаджиева Л.К., Котенко В.В., Румянцев К.Е. Нейролингвистическая информационная идентификация интеллектуальных систем // Известия ЮФУ. Технические науки. Ростов–на–Дону: Издательство Южного федерального университета, №3 (239). 2024 г. – С. 33-44.

7. Котенко В.В., Хаджиева Л.К. Аутентификация и системы разграниченного доступа пользовательского уровня как меры защиты информации в банках // Сборник статей XII Всероссийской научно-практической конференции «Молодежь, наука, инновации», Грозный, 18 октября 2023 г., стр. 72-76.

8. Litvinova T. Authorship attribution of russian social media texts: does the volume of data favor idiolect identification? / Lecture Notes in Networks and Systems. – 2022. – T. 315 LNNS. – P. 352-362.

9. Symmetric Multi-Scale Residual Network Ensemble with Weighted Evidence Fusion Strategy for Facial Expression Recognition. / Juan Liu, Min Hu, Ying Wang, Zhong Huang, Julang Jiang // Symmetry. – 2023. – 15 (6). – P. 1228. – https://doi.org/10.3390/sym15061228

10. Ямченко Ю.В. Методы решения задач аутентификации и идентификации пользователя на основе анализа клавиатурного почерка // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия Приборостроение. – 2020. – № 1 (130). – С. 124-139.

11. Куртукова, А. В. Разработка интеллектуальной системы для идентификации автора исходного кода на основе нейронных сетей / А. В. Куртукова. — Текст: непосредственный // Молодой ученый. — 2020. — № 40 (330). — С. 2-3.

12. Куртукова А.В., Романов А.С., Соболев А.А. Воздействие корпоративных стандартов разработки на идентификацию автора исходного кода // Электронные средства и системы управления. Материалы докладов Международной научно-практической конференции. 2020. № 1-2. С. 140-142.

13. Куртукова А.В., Романов А.С. Проблема искусственно сгенерированных исходных кодов в задаче идентификации автора программы // Сборник избранных статей научной сессии ТУСУР. 2022. № 1-2. С. 131-134.

14. Куртукова А.В., Романов А.С., Федотова А.М., Шелупанов А.А. Архитектура интеллектуальной системы для идентификации автора исходного кода// Доклады Томского государственного университета систем управления и радиоэлектроники. 2022. Т. 25. № 3. С. 39-44.

15. Кетермина Т.С., Тагиров Т.М. Элементы искусственного интеллекта в решении задач анализа текстов // Computational nanotechnology. 2022 N. 9. №2. С. 35-44. DOI: 10. 33693/2313-223X-2022-9-2-35-44.

16. Черкасов А.Н., Туркин Е.А. Выбор оптимальной архитектуры искусственной нейронной сети для задачи классификации текстов // Ежеквартальный рецензируемый, реферируемый научный журнал «Вестник АГУ». Выпуск 1 (276) 2021. С. 62-66.

17. Уздяев М.Ю. Распознавание агрессивных действий с использованием нейросетевых архитектур 3d-cnn. // Известия ТулГУ. Технические науки. 2020. Выпуск 2 С. 316- 329.

18. Батраева И.А., Нарцев А. Д., Лезгян А.С. Использование анализа семантической сложности слов при определении задач определения жанровых принадлежностей текстов, методов глубокого обучения. // Вестник томского государственного университета № 50 2020. С. 14-21.

19. Частикова В.А., Казачев К.В., Гуляй В.Г. Методы обработки естественного языка в решении задач обнаружения атак социальной инженерии. // Ежеквартальный рецензируемый, реферируемый научный журнал «Вестник АГУ». Выпуск 1 (291) 2021. С. 95-107.

20. Глазкова А.В. Сравнение нейросетевых моделей для классификации текстовых фрагментов, содержащих биографическую информацию. // Тюменский государственный университет. Т. 32. №2 С. г. Тюмень, 625003, Россия 2019 С. 65-69.

## References

1. Kotenko V. V., Rumyantsev K. Ye., Khadzhiyeva L. K. Otsenka vozmozhnostey neyrolingvisticheskoy identifikatsii sistem iskusstvennogo intellekta // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere, Izdatel'skiy tsentr FGAOU VO «YUUrGU (NIU)» № 2(52) / 2024 g. – S – 13-24.

2. Kotenko V.V. Tekhnologii informatsionnogo analiza pol'zovatel'skogo urovnya telekommunikatsionnykh sistem. Uchebnoye posobiye // Rostov-na-Donu – Taganrog: Izdatel'stvo Yuzhnogo federal'nogo universiteta, 2019. – 194 s.

3. Kotenko V.V., Rumyantsev K.Ye. Teoriya informatsii. Uchebnoye posobiye // Rostov-na-Donu – Taganrog: Izdatel'stvo Yuzhnogo federal'nogo universiteta, 2018. – 239 s.

4. Kotenko V.V. Teoriya virtualizatsii i zashchita telekommunikatsiy: monografiya – Taganrog: Izd-vo TTI YUFU, 2011. – 236 s.

5. Kotenko V.V. Rumyantsev K.Ye., Kotenko S.V. Metodologiya identifikatsionnogo analiza infokommunikatsionnykh sistem. Monografiya. – Rostov–na–Donu: Izdatel'stvo Yuzhnogo federal'nogo universiteta, 2014. – 315 s.

6. Khadzhiyeva L.K., Kotenko V.V., Rumyantsev K.Ye. Neyrolingvisticheskaya informatsionnaya identifikatsiya intellektual'nykh sistem // Izvestiya YUFU. Tekhnicheskiye nauki. Rostov–na–Donu: Izdatel'stvo Yuzhnogo federal'nogo universiteta, №3 (239). 2024 g. – S. 33-44.

7. Kotenko V.V., Khadzhiyeva L.K. Autentifikatsiya i sistemy razgranichennogo dostupa pol'zovatel'skogo urovnya kak mery zashchity informatsii v bankakh // Sbornik statey XII Vserossiyskoy nauchno-prakticheskoy konferentsii «Molodezh', nauka, innovatsii», Groznyy, 18 oktyabrya 2023 g., str. 72-76.

8. Litvinova T. Authorship attribution of russian social media texts: does the volume of data favor idiolect identification? / Lecture Notes in Networks and Systems. – 2022. – T. 315 LNNS. – P. 352-362.

9. Symmetric Multi-Scale Residual Network Ensemble with Weighted Evidence Fusion Strategy for Facial Expression Recognition. / Juan Liu, Min Hu, Ying Wang, Zhong Huang, Julang Jiang // Symmetry. – 2023. – 15 (6). – P. 1228. – https://doi.org/10.3390/sym15061228

10. Yamchenko YU.V. Metody resheniya zadach autentifikatsii i identifikatsii pol'zovatelya na osnove analiza klaviaturnogo pocherka // Vestnik Moskovskogo gosudarstvennogo tekhnicheskogo universiteta im. N.E. Baumana. Seriya Priborostroyeniye. – 2020. – № 1 (130). – S. 124-139.

11. Kurtukova, A. V. Razrabotka intellektual'noy sistemy dlya identifikatsii avtora iskhodnogo koda na osnove neyronnykh setey / A. V. Kurtukova. — Tekst: neposredstvennyy // Molodoy uchenyy. — 2020. — № 40 (330). — S. 2-3.

12. Kurtukova A.V., Romanov A.S., Sobolev A.A. Vozdeystviye korporativnykh standartov razrabotki na identifikatsiyu avtora iskhodnogo koda // Elektronnyye sredstva i sistemy upravleniya. Materialy dokladov Mezhdunarodnoy nauchno-prakticheskoy konferentsii. 2020. № 1-2. S. 140-142.

13. Kurtukova A.V., Romanov A.S. Problema iskusstvenno sgenerirovannykh iskhodnykh kodov v zadache identifikatsii avtora programmy // Sbornik izbrannykh statey nauchnoy sessii TUSUR. 2022. № 1-2. S. 131-134.

14. Kurtukova A.V., Romanov A.S., Fedotova A.M., Shelupanov A.A. Arkhitektura intellektual'noy sistemy dlya identifikatsii avtora iskhodnogo koda// Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki. 2022. T. 25. № 3. S. 39-44.

15. Ketermina T.S., Tagirov T.M. Elementy iskusstvennogo intellekta v reshenii zadach analiza tekstov // Computational nanotechnology. 2022 N. 9. №2. S. 35-44. DOI: 10. 33693/2313-223KH-2022-9-2-35-44.

16. Cherkasov A.N., Turkin Ye.A. Vybor optimal'noy arkhitektury iskusstvennoy neyronnoy seti dlya zadachi klassifikatsii tekstov // Yezhekvartal'nyy retsenziruyemyy, referiruyemyy nauchnyy zhurnal «Vestnik AGU». Vypusk 1 (276) 2021. S. 62-66.

17. Uzdyayev M.YU. Raspoznavaniye agressivnykh deystviy s ispol'zovaniyem neyrosetevykh arkhitektur 3d-cnn. // Izvestiya TulGU. Tekhnicheskiye nauki. 2020. Vypusk 2 S. 316- 329.

18. Batrayeva I.A., Nartsev A. D., Lezgyan A.S. Ispol'zovaniye analiza semanticheskoy slozhnosti slov pri opredelenii zadach opredeleniya zhanrovykh prinadlezhnostey tekstov, metodov glubokogo obucheniya. // Vestnik tomskogo gosudarstvennogo universiteta № 50 2020. S. 14-21.

19. Chastikova V.A., Kazachev K.V., Gulyay V.G. Metody obrabotki yestestvennogo yazyka v reshenii zadach obnaruzheniya atak sotsial'noy inzhenerii. // Yezhekvartal'nyy retsenziruyemyy, referiruyemyy nauchnyy zhurnal «Vestnik AGU». Vypusk 1 (291) 2021. S. 95-107.

20. Glazkova A.V. Sravneniye neyrosetevykh modeley dlya klassifikatsii tekstovykh fragmentov, soderzhashchikh biograficheskuyu informatsiyu. // Tyumenskiy gosudarstvennyy universitet. T. 32. №2 S. g. Tyumen', 625003, Rossiya 2019 S. 65-69.

---

**КОТЕНКО Владимир Владимирович,** кандидат технических наук, доцент кафедры «Информационная безопасность телекоммуникационных систем». Институт компьютерных технологий и информационной безопасности ЮФУ. 347922, Ростовская область, г. Таганрог, ул. Чехова, 2. E-mail: kotenkovv@sfedu.ru

**РУМЯНЦЕВ Константин Евгеньевич,** доктор технических наук, профессор, заведующий кафедрой «Информационная безопасность телекоммуникационных систем». Институт компьютерных технологий и информационной безопасности ЮФУ. 347922, Ростовская область, г. Таганрог, ул. Чехова, 2. E-mail: rumyancev@sfedu.ru

**ХАДЖИЕВА Лаура Куйраевна,** соискатель кафедры «Информационная безопасность телекоммуникационных систем». Институт компьютерных технологий и информационной безопасности ЮФУ. 347922, Ростовская область, г. Таганрог, ул. Чехова, 2.; старший преподаватель кафедры «Информатика и вычислительная техника». Грозненский государственный нефтяной технический университет имени академика М.Д. Миллионщикова. 364061, Чеченская Республика., г. Грозный, пр. Х. Исаева, 100. E-mail: laura.hadjieva3009@mail.ru

**KOTENKO Vladimir Vladimirovich,** Candidate of Technical Sciences, Associate Professor of the Department of Information Security of Telecommunication Systems. Institute of Computer Technologies and Information Security of SFedU. 347922, Rostov Region, Taganrog, Chekhov St., 2. E-mail: kotenkovv@sfedu.ru.

**RUMYANTSEV Konstantin Evgenievich,** Doctor of Technical Sciences, Professor, Head of the Department of Information Security of Telecommunication Systems. Institute of Computer Technologies and Information Security of SFedU. 347922, Rostov Region, Taganrog, Chekhov St., 2. E-mail: rumyancev@sfedu.ru

**KHADZHIEVA Laura Kuiraevna,** applicant, Department of Information Security of Telecommunication Systems. Institute of Computer Technologies and Information Security, SFedU. 347922, Rostov Region, Taganrog, Chekhov St., 2; senior lecturer, Department of Computer Science and Engineering. Grozny State Oil Technological University named after Academician M.D. Millionshchikov. 364061, Chechen Republic, Grozny, Kh. Isaev Ave., 100. E-mail: laura.hadjieva3009@mail.ru

УДК 004.942:519.23/.25 Вестник УрФО № 3(53) / 2024, с. 44–53

**Медведев М. А.**

DOI: 10.14529/secur240305

# *ИССЛЕДОВАНИЕ И ОЦЕНКА МЕТОДОВ АВТОМАТИЗАЦИИ СБОРА И ОБРАБОТКИ СЕТЕВОГО ТРАФИКА ДЛЯ ЗАДАЧ КОНТЕНТ-ФИЛЬТРАЦИИ*

*Цель данной статьи – проведение оценки эффективности методов автоматизации сбора и обработки сетевого трафика. В условиях постоянно растущих объемов данных и увеличивающихся требований к их обработке предложен алгоритм, способный автоматически собирать и обрабатывать сетевой трафик с удаленных узлов, минимизируя задержки и повышая производительность системы. Основное внимание уделено трем ключевым аспектам: исследованию способов преобразования сетевого трафика, определению критериев для создания датасета в области семантической контент-фильтрации и оценке эффективности предложенных методов автоматизации. В рамках исследования выполнено преобразование сетевого трафика с использованием методов нормализации, фильтрации нерелевантных данных и разделения на сессии. Для оценки эффективности методов были предложены и использованы четыре критерия: масштабируемость, точность и качество данных, скорость обработки, а также управление потоками данных.*

*Новизна работы заключается в разработке стандартизированного подхода для сбора и обработки сетевого трафика, что способствует повышению точности моделей машинного обучения в задачах семантической контент-фильтрации. Предлагаемые результаты указывают возможные пути улучшения в рамках автоматизации обработки больших объемов сетевого трафика с высокой производительностью.*

***Ключевые слова:*** *автоматизация сбора сетевого трафика, преобразование трафика, нормализация данных, семантическая контент-фильтрация, масштабируемость, точность данных, фильтрация трафика, управление данными.*

# *RESEARCH AND EVALUATION OF METHODS FOR AUTOMATING NETWORK TRAFFIC COLLECTION AND PROCESSING FOR CONTENT FILTERING TASKS*

*The aim of this paper is to assess the effectiveness of methods for automating network traffic collection and processing. In the context of continuously increasing data volumes and growing demands for processing, an algorithm capable of automatically collecting and processing network traffic from remote nodes is proposed, minimizing delays and enhancing system performance. The focus is on three key aspects: investigating methods for transforming network traffic, defining criteria for creating datasets in semantic content filtering, and evaluating the effectiveness of the proposed automation methods. The study involved transforming network traffic using methods of normalization, irrelevant data filtering, and session separation. Four criteria were proposed and used to assess the effectiveness of the methods: scalability, data accuracy and quality, processing speed, and data flow management.*

*The novelty of the work lies in the development of a standardized approach for collecting and processing network traffic, which contributes to improving the accuracy of machine learning models in semantic content filtering tasks. The proposed results indicate possible improvements in automating the processing of large volumes of network traffic with high performance.*

***Keywords:*** *automation of network traffic collection, traffic transformation, data normalization, semantic content filtering, scalability, data accuracy, traffic filtering, data management.*

**Введение**

С каждым годом объем сетевого трафика неуклонно растет, что ставит перед специалистами в области сетевой безопасности и управления данными задачу разработки эффективных методов автоматизации сбора и обработки сетевого трафика. Актуальность данного исследования обусловлена необходимостью повышения точности и скорости обработки данных, что напрямую влияет на своевременное обнаружение угроз и аномалий в сетях. Автоматизация этих процессов позволяет не только улучшить производительность систем, но и позволит существенно снизить нагрузку на вычислительные мощности, что особенно важно для современных крупных сетей и облачных инфраструктур.

Цель данного исследования – провести оценку эффективности методов автоматизации сбора и обработки сетевого трафика для повышения точности, масштабируемости и скорости обработки данных.

Для достижения цели были поставлены следующие задачи:

1) исследовать и проанализировать существующие способы преобразования сетевого трафика;
2) определить критерии для создания датасета, используемого в задачах семантической контент-фильтрации;
3) оценить эффективность методов автоматизации сбора и обработки сетевого трафика, опираясь на предложенные критерии: масштабируемость, точность и качество данных, скорость и управление потоками данных.

Ряд исследований в области сетевой безопасности и обработки трафика демонстрируют необходимость применения методов машинного обучения и алгоритмов фильтра-

ции для повышения точности анализа трафика. Исследования Чжао и Ву [1] предложили подход на основе подпространств для обнаружения аномалий в кампусных сетях, который показал высокую эффективность при работе с большими объемами данных. В то же время, работы Вэйбао Чжана и Жоан П. Ласаро [2] подробно анализируют методы обнаружения аномалий, используя статистические методы и машинное обучение. Однако большинство решений все еще сталкиваются с проблемами масштабируемости и управлением потоками данных в реальном времени, что делает задачу автоматизации сбора и обработки трафика актуальной и незавершенной. В исследовании Гебрей, Ванг и Ли [3] особое внимание уделяется критическим аспектам извлечения и маркировки данных для машинного обучения в системах обнаружения атак в сетях IoT. Авторы подробно описывают методологии, направленные на повышение точности и эффективности моделей машинного обучения при работе с изменчивыми и большими объемами данных IoT. В работе Адила и Альфоуди [4] исследуется применение алгоритмов машинного обучения для классификации трафика в сетях с программно-конфигурируемой инфраструктурой (SDN). Исследование Фана и коллег [5] предлагает новый подход к анализу трафика IoT с помощью «отпечатков трафика», основанных на анализе переходов в пакетных данных. Авторы [5] рассматривают уникальные паттерны трафика различных устройств IoT, что может помочь в оптимизации и улучшении сетевой безопасности.

Основная проблема, которую решает данное исследование, заключается в разработке методов автоматизации сбора и обработки сетевого трафика с учетом масштабируемости, точности данных и скорости их обработки. Предполагается, что применение программного зеркалирования и методов нормализации данных на уровне удаленных узлов позволит существенно улучшить производительность системы и снизить время отклика на потенциальные угрозы.

Для решения поставленных задач был разработан алгоритм автоматизации сбора сетевого трафика, основанный на использовании программного зеркалирования, фильтрации нерелевантных данных и нормализации трафика. Применялись методы фильтрации трафика, разделения данных на сессии и создания стандартизированных CSV-файлов для повышения точности классификации данных. Оценка эффективности предложенных методов была проведена на основе четырех ключевых критериев: масштабируемость, точность и качество данных, скорость обработки и управление потоками данных.

Статья состоит из нескольких разделов. В первой части исследуются существующие методы преобразования сетевого трафика и проводится их анализ с точки зрения масштабируемости и точности. Во второй части описываются критерии, которые были использованы для создания датасета для задач семантической контент-фильтрации. В третьей части подробно рассматриваются разработанные методы автоматизации и их оценка по каждому из критериев. В заключении представлены выводы о проделанной работе.

## Исследование способов преобразования сетевого трафика

Сложность и динамика современного сетевого трафика требуют от исследователей не только глубокого понимания существующих подходов и технологий, но и разработки новых алгоритмов, способных адекватно реагировать на постоянные изменения в сетевой активности. Исследование нацелено на решение проблемы эффективного сбора и обработки данных, что позволит формировать более качественные наборы данных на основании, которых можно проводить дальнейшее исследование сетевого трафика. Перейдем к рассмотрению основных научных статей, которые затрагивают аспекты автоматизации сбора и обработки данных.

Статья Сяофэн Чжао и Цюйбин Ву [1] представляет собой значимый вклад в область обнаружения аномалий в сетевом трафике, используя методы анализа подпространства. Этот подход основывается на выделении основных компонент трафика, которые могут указывать на нестандартное или аномальное поведение. Метод анализа подпространства может быть формализован через применение техник линейной алгебры для сокращения размерности данных [1]. Основное предположение состоит в том, что большинство нормальных данных сетевого трафика находятся в низкоразмерном подпространстве, в то время как аномалии будут проявляться в виде отклонений от этого подпространства [1]. Математически это можно описать следующей моделью (формула 1):

$$X = T\sum V^T + E, \quad (1)$$

где $X$ – исходные данные, $T$ и $V$ – матрицы, описывающие подпространства, $\Sigma$ – диагональная матрица сингулярных значений, указывающая на важность каждого подпространства, и $E$ – матрица ошибок или шума.

Применение данной методики в контексте мониторинга сетевого трафика позволяет обнаруживать аномалии путем анализа резидуальных компонент $E$, которые не укладываются в основное подпространство [1]. Эта методика позволяет не только обнаруживать существующие угрозы, но и прогнозировать потенциальные проблемы, обеспечивая тем самым более высокий уровень предсказуемости и контроля за сетевой средой.

В статье Вэйбао Чжана и Жоан П. Ласаро [2] представлен широкий обзор методов, применяемых в современной сетевой безопасности для анализа трафика и обнаружения аномалий. Авторы детально изучают и сравнивают различные подходы – от традиционных статистических методов до современных алгоритмов машинного обучения. Это исследование помогает определить, какие методы наиболее эффективны в различных операционных условиях, а какие могут быть менее результативными.

Статистические методы, как первые инструменты анализа сетевого трафика, включают вычисление таких метрик, как среднее значение, стандартное отклонение и коэффициенты корреляции между типами трафика. Эти простые, но важные показатели позволяют выявлять отклонения в сетевом поведении. Например, стандартное отклонение, рассчитываемое по следующей формуле (формула 2), помогает оценивать степень вариации данных:

$$\sigma = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}\left(x_i - \mu\right)^2}, \quad (2)$$

где $\sigma$ – стандартное отклонение, $N$ – количество измерений, $x_i$ – значение каждого измерения, $\mu$ – среднее значение измерений.

Авторы [2] акцентируют внимание на понимании преимуществ и недостатков каждого подхода, что позволяет более точно настраивать системы защиты, улучшать процессы обработки данных и обеспечивать высокую безопасность сетевых ресурсов.

Исследование Хайелома Гебрея, Юна Ванга и Фагена Ли [3] посвящено важнейшим аспектам извлечения и маркировки данных в сетях Интернета вещей (IoT), что играет ключевую роль в разработке и внедрении систем обнаружения атак на основе машинного обучения. Главная проблема заключается в обеспечении высокой точности и надежности данных, которые поступают на вход алгоритмов машинного обучения, что важно для своевременного и точного обнаружения аномалий и угроз в условиях динамически изменяющегося и разнообразного трафика IoT [3].

Исследователи [3] акцентируют внимание на том, что для успешной работы алгоритмов необходимо обеспечить точный захват данных, соответствующих специфическим задачам. Одним из подходов, предложенных авторами [3], является фильтрация трафика на основе заранее определенных критериев, что позволяет существенно снизить объем данных для обработки и, как следствие, повысить скорость и точность последующего анализа [3]. Например, один из применяемых методов может быть представлен в виде алгоритма классификации (формула 3):

$$y = f(x \mid \theta), \quad (3)$$

где $y$ – метка класса, $x$ – входные данные, $\theta$– параметры модели.

Методики, разработанные для извлечения и маркировки данных в сетях IoT, позволят улучшить качество данных, используемых для обучения моделей машинного обучения, что напрямую скажется на эффективности систем обнаружения атак [3].

Статья Самаха Адила и Али Саида Альфоуди [4] посвящена исследованию применения различных алгоритмов машинного обучения для классификации сетевого трафика в средах с программно-конфигурируемой инфраструктурой (SDN). Одним из центральных аспектов анализа работы авторов [4] является вычисление метрик качества классификации, таких как точность (Accuracy), точность по классу (Precision), полнота (Recall) и F1-мера. Эти метрики рассчитываются по следующим формулам (формулы 4, 5, 6, 7):

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}, \quad (4)$$

$$Precision = \frac{TP}{TP + FP}, \quad (5)$$

$$Recall = \frac{TP}{TP + FN}, \quad (6)$$

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}, \quad (7)$$

где TP – истинно положительные, TN – истинно отрицательные, FP – ложно положительные, FN – ложно отрицательные результаты.

Результаты исследования демонстрируют, что различные алгоритмы машинного обучения могут эффективно применяться для улучшения управления сетевым трафиком и обеспечения безопасности в SDN. Это исследование предоставляет важные сведения для разработки интеллектуальных и автоматизированных систем управления трафиком, способствующих повышению общей производительности и безопасности сетевой инфраструктуры [4].

В статье Мингруй Фана [5] представлен инновационный метод анализа трафика, основанный на изучении переходных моделей в пакетных данных, с целью создания уникальных «отпечатков трафика» для устройств Интернета вещей (IoT). Эти отпечатки позволяют идентифицировать и классифицировать различные типы устройств IoT на основе их характерных паттернов трафика [5]. Метод основан на анализе изменений в последовательностях, передаваемых и получаемых данных, с использованием статистических и машинно-обучаемых моделей. Это позволяет генерировать детализированные профили каждого типа устройства, где «отпечатки» формируются на основе частоты и последовательности передач пакетов данных. Например, вероятность перехода между состояниями вычисляется по формуле (формула 8):

$$p_{ij} = \frac{n_{ij}}{\sum_k n_{ik}}, \quad (8)$$

где $P_{ij}$ – вероятность перехода от состояния i к состоянию j, $n_{ij}$ – количество переходов от i к j, а $\sum_k n_{ik}$ – общее количество переходов из состояния i.

Исследование подчеркивает необходимость детализированного анализа трафика в условиях постоянно растущего числа подключенных устройств в современных сетях [5].

В данной главе подробно рассмотрены различные подходы и методы преобразования сетевого трафика, направленные на повышение эффективности мониторинга, анализа и управления сетевыми ресурсами. Авторы предложили методы, способствующие улучшению сетевой безопасности и более рациональному использованию ресурсов. Проведенный анализ алгоритмов позволил выявить ключевые критерии, которые могут служить основой для разработки алгоритма автоматизации сбора и обработки сетевого трафика. Эти критерии будут использоваться для дальнейшего совершенствования методов анализа и обработки данных, что позволит повысить точность и оперативность обнаружения угроз в сети.

### Формирование критериев для создания датасета

Следующий этап настоящего исследования будет включать сравнительный анализ подходов определенных в исследованиях авторов с целью формирования критериев для создания датасета в области семантической контент-фильтрации с последующей разработкой алгоритма автоматизации сбора и обработки трафика. Проведем сравнительный анализ описанных выше исследований (таблица 1), для выделения основных характеристик, целей и задач.

Таблица 1 представляет методы, цели и решаемые задачи, описанные в каждой статье, демонстрируя разнообразие методов, направленных на улучшение сбора и обработки сетевого трафика. В первой, четвертой и пятой статьях представлены специализированные алгоритмы для решения задач, как обнаружение аномалий, классификация трафика и создание «отпечатков» трафика. Вторая статья представляет обзор существующих методов, предоставляя сравнительный анализ различных подходов. В третьей статье представлены методы совершенствования процессов извлечения и маркировки данных, а также оценка методов аутентификации. Вторая и третья статьи – вносят предложения для обучения и оценки технологий, что повышает их эффективность и углубляет понимание методов.

На основе проведенного анализа можно выделить следующие критерии, необходимые для автоматизации сбора и обработки сетевого трафика:

1) критерий масштабируемости – способность системы эффективно обрабатывать увеличивающиеся объемы данных без снижения производительности;

*Таблица 1*

**Основные характеристики и методы**

| п/п | Название статьи | Методы и подходы | Цели исследования | Основные задачи |
|---|---|---|---|---|
| 1 | Subspace-Based Anomaly Detection for Large-Scale Campus Network Traffic | Математический анализ подпространств | Обнаружение аномалий в кампусных сетях | Выявление аномалий в сетевом трафике |
| 2 | A Survey on Network Security Traffic Analysis and Anomaly Detection Techniques | Обзор и сравнение существующих методов | Обзор текущих и перспективных технологий анализа трафика и обнаружения аномалий | Сравнительный анализ методов обнаружения аномалий |
| 3 | Traffic Data Extraction and Labeling for Machine Learning Based Attack Detection in IoT Networks | Методы извлечения и маркировки данных | Улучшение машинного обучения для обнаружения атак в IoT сетях | Извлечение и маркировка данных для обучения моделей |
| 4 | Traffic Data Classification in SDN Network Based on Machine Learning Algorithms | Алгоритмы машинного обучения для классификации трафика | Оптимизация безопасности и управления в SDN через классификацию трафика | Классификация сетевого трафика в SDN |
| 5 | Traffic Fingerprints for Homogeneous IoT Traffic Based on Packet Payload Transition Patterns | Анализ паттернов переходов в пакетных данных | Создание уникальных «отпечатков» трафика для идентификации устройств IoT | Формирование отпечатков IoT трафика на основе анализа пакетов |

2) критерий точности и качества данных – необходимость точного захвата, классификации и маркировки данных для их последующего анализа и использования в моделях машинного обучения;
3) критерий скорости – возможность системы обрабатывать и классифицировать данные в режиме реального времени;
4) критерий управления и обработки данных – процессы фильтрации, агрегации и хранения, упрощающие дальнейший анализ и снижающие нагрузку на системы хранения.

Разработка алгоритма автоматизации сбора и обработки сетевого трафика требует тщательного понимания характеристик современных сетевых инфраструктур, которые постоянно сталкиваются с увеличением объемов данных. Выделенные критерии позволят эффективно структурировать процесс создания алгоритмов, ориентированных на решение реальных технических задач. Анализ рисков и проблем, основанный на этих критериях, поможет глубже оценить потенциальные угрозы и разработать оптимальные стратегии для их минимизации.

**Оценка эффективности методов автоматизации сбора и обработки сетевого трафика**

Разработка методов автоматизации сбора и обработки сетевого трафика является важной задачей в условиях роста объемов данных и повышенных требований к их обработке. В работе оцениваются предложенные методы на основе четырех критериев. Рассматриваются такие подходы, как программное зеркалирование и обработка данных с удаленных узлов.

Программное зеркалирование является инструментом для захвата трафика, позволяя дублировать данные с удаленных узлов и передавать их на центральный сервер для последующей обработки. Это особенно эффективно для распределенных сетей, где центральный сервер не имеет прямого доступа ко всем узлам. Такой подход снижает нагрузку на удаленные узлы и обеспечивает централизованное управление трафиком. Схема подключения удаленных узлов к серверу показана на рисунке 1.

Данный подход повышает точность сбора данных и ускоряет их обработку благодаря первичной фильтрации и нормализации на

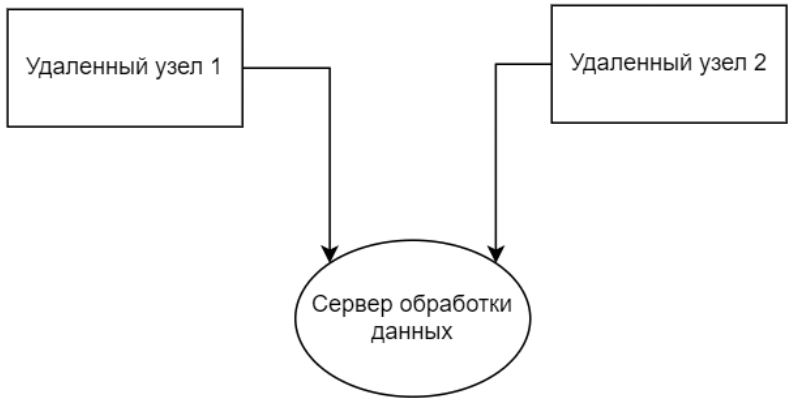


Рис. 1. Схема подключений

удаленных узлах. Распределение вычислительных ресурсов между узлами и сервером оптимизирует процесс обработки трафика, что особенно важно при работе с большими объемами данных (формула 10) [6]:

$$T_{total} = \sum_{i=1}^{n} T_i, \quad (10)$$

где $T_{total}$ – общий объем трафика, который обрабатывается сервером, $T_i$ – объем трафика, поступающий с каждого удаленного узла i, а n – количество удаленных узлов.

Масштабируемость системы является способность системы адаптироваться к увеличению объемов трафика без потери производительности. Применение программного зеркалирования распределяет нагрузку между удаленными узлами и центральным сервером, позволяя системе оперативно обрабатывать данные даже при росте объема трафика, без существенных задержек.

После передачи данных на основной сервер с помощью программного зеркалирования применяется метод обработки трафика с удаленных узлов, представленный на рисунке 2.

Процесс включает в себя:

1) извлечение пакетов из протокола TZSP, используемого для передачи захваченного трафика, который после служит основой для дальнейшей обработки;
2) удаление локальных и нерелевантных адресов, что сокращает объем данных для анализа и оптимизирует обработку;
3) нормализация пакетов, стандартизирующая формат данных и преобразующая их в pcap для совместимости с аналитическими инструментами;
4) разделение трафика на сессии, упрощающее классификацию и анализ сетевых данных;
5) создание CSV-формата, который структурирует данные с разделением на категории True и False, улучшая их пригодность для обучения моделей машинного обучения.

Процесс нормализации пакетов и их разделения можно представить по следующей формуле (11) [7]:

$$S = \{p_1, p_2, ..., p_n\}, \quad T_{true}, T_{false} \subset S, \quad (11)$$

где S – множество пакетов в сессии, $T_{true}$ – подмножество нормальных пакетов, и $T_{false}$ – подмножество аномальных пакетов.

Точность захвата и качество данных являются ключевыми факторами успешного анализа сетевого трафика. Основные методы – это нормализация, фильтрация нерелевантной информации и разделение трафика на сессии (рисунок 2) – минимизируют ошибки и упрощают анализ.

Пусть D – исходный объем данных, поступающих в систему. Фильтрация и нормализация уменьшают объем данных до D', где (формула 12):

$$D' = D - F(D), \quad (12)$$

где F(D) – функция, удаляющая нерелевантные или дублирующиеся данные.

Для упрощения обработки данные разделяются на сессии $S_i$, где i – номер сессии, а n – общее количество сессий (формула 13):

$$S = \{S_1, S_2, ..., S_n\}, \quad (13)$$

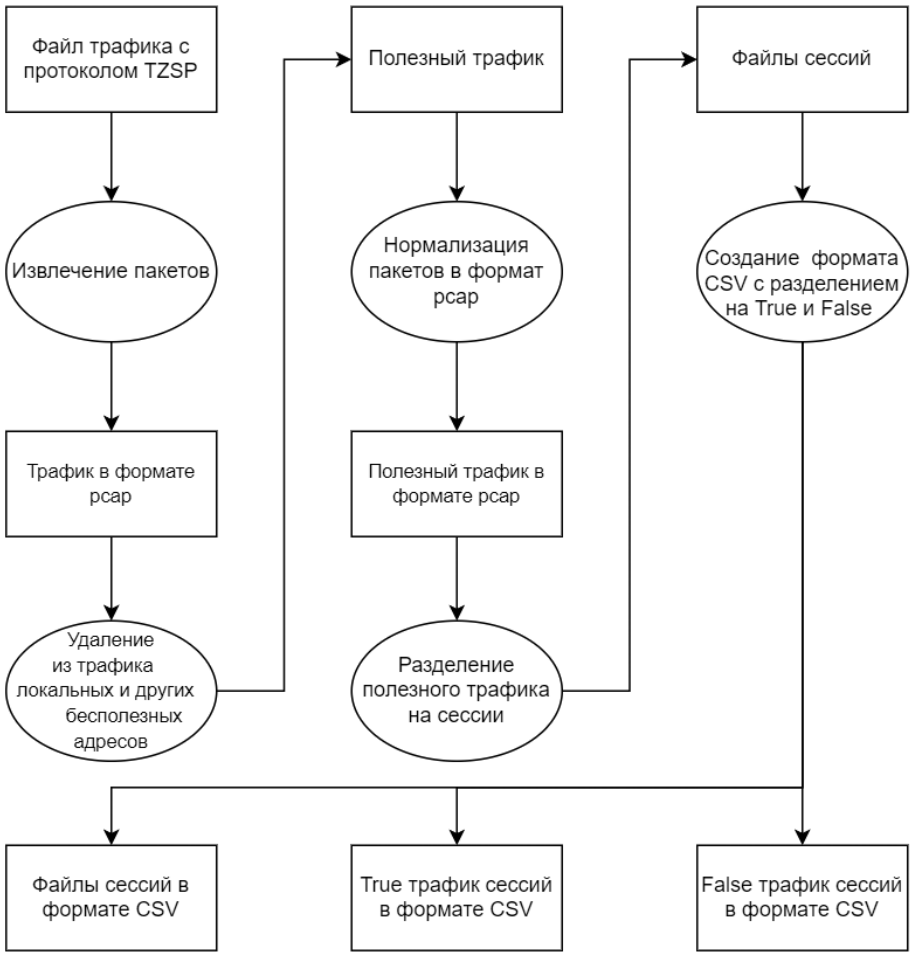


Рис. 2. Алгоритм сбора и обработки трафика

Каждая сессия нормализуется и преобразуется в формат CSV, что упрощает дальнейшую обработку.

Эффективность фильтрации оценивается через временную сложность $O_n(f(D))$, где $D$ – исходный объем данных. Общая сложность нормализации и фильтрации может быть выражена как (формула 14):

$$O_n(f(D)) = O_n(D \log D), \qquad (14)$$

Это предполагает использование эффективных алгоритмов, что существенно сокращает объем данных и время на их обработку.

Создание стандартизированного формата CSV с разделением на True и False трафик улучшает качество данных для машинного обучения. Пусть $X$ – множество всех пакетов данных, тогда каждый пакет $x \in X$ классифицируется как True или False, что формально выражается так (формула 15):

$$\begin{aligned} x \in T \quad & \text{если } x \text{ соответствует нормальному трафику} \\ x \in F \quad & \text{если } x \text{ соответствует аномальному трафику} \end{aligned} \qquad (15)$$

Точность классификации моделей машинного обучения измеряется метрикой точности (формула 16) [4]:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}, \qquad (16)$$

где $TP$ – истинно положительные, $TN$ – истинно отрицательные, $FP$ – ложно положительные, $FN$ – ложно отрицательные результаты. Чем выше точность захвата и фильтрации данных, тем больше $TP$ и $TN$, что повышает общую точность модели.

Скорость обработки, управление потоками и эффективная обработка трафика играют

ключевую роль в обеспечении надежной и производительной системы автоматизации сбора трафика. Эти аспекты работают совместно, позволяя системе быстро реагировать на угрозы, минимизировать задержки и снижать нагрузку на ресурсы. Внедрение методов программного зеркалирования и обработки трафика на удаленных узлах позволит сократить задержки при передаче данных на сервер и их последующей обработке [6].

Управление потоками данных и их эффективная обработка дополняют скорость системы, уменьшая нагрузку на сервер за счет фильтрации нерелевантных данных на этапе сбора [8]. Фильтрация удаляет локальные и незначимые адреса, сокращая объем данных и снижая требования к системам хранения и анализа [8]. Нормализация пакетов позволит ускорить процесс обработки и стандартизировать данные для дальнейшего анализа и классификации.

Процесс обработки и управления потоками можно описать математической моделью (формула 17) [8]:

$$T_{proc} = \frac{\sum_{i=1}^{n} P_i - F}{C_s}, \qquad (17)$$

где $T_{proc}$ – общее время обработки, $P_i$ – объем трафика с узла i, F – объем отфильтрованных данных, $C_s$ – вычислительная мощность системы. Фильтрация на удаленных узлах снижает объем данных, передаваемых на сервер, что уменьшает время обработки и увеличивает скорость системы [8].

Объединение методов управления и обработки данных с высокой скоростью позволит системе эффективно справляться с увеличением объемов трафика. Ускоренная обработка и управление потоками не только снизят нагрузку на сервер, но и обеспечат быструю реакцию на потенциальные угрозы, что особенно важно при работе с большими объемами данных.

На основании проведенного исследования автоматизации сбора и обработки сетевого трафика сделаны выводы по четырем ключевым критериям: масштабируемость, точность, скорость и управление данными. Программное зеркалирование для распределенной обработки на удаленных узлах демонстрирует высокую масштабируемость, позволяя системе эффективно справляться с ростом трафика, поддерживая производительность и снижая нагрузку на центральные ресурсы. Точность и качество данных обеспечиваются нормализацией, фильтрацией и разделением трафика на сессии, с последующей стандартизацией в формате CSV для улучшения анализа. Скорость обработки возрастет благодаря фильтрации на удаленных узлах, что сократит объем передаваемых данных и уменьшит задержки. Эффективное управление потоками будет достигаться за счет ранней фильтрации и нормализации, что снизит нагрузку на системы хранения и вычислительные ресурсы. Внедрение данных критериев позволяет разработать надежный и эффективный алгоритм автоматизации сбора и обработки трафика.

**Заключение**

Целью данного исследования являлась оценка эффективности методов автоматизации сбора и обработки сетевого трафика для повышения точности, масштабируемости и скорости обработки данных. В ходе работы были решены следующие задачи: проведён анализ существующих методов преобразования сетевого трафика, определены критерии для создания датасета, используемого в задачах семантической контент-фильтрации, и выполнена оценка эффективности методов автоматизации на основе предложенных критериев – масштабируемости, точности и качества данных, скорости, управления потоками и обработкой данных.

Анализ методов программного зеркалирования, нормализации и фильтрации трафика на удалённых узлах показал их высокую эффективность при увеличении объёмов данных. Эти подходы обеспечат точный захват, минимизируют нагрузку на центральный сервер и поспособствуют улучшению масштабируемости системы.

Поставленные задачи исследования были достигнуты: предложенный алгоритм улучшил точность обработки данных, снизил задержки и повысил масштабируемость системы. Кроме того, выполнена задача по формированию критериев оценки методов для задач семантической контент-фильтрации. Перспективы дальнейшего развития системы связаны с внедрением потоковой обработки данных в реальном времени, что позволит ещё более эффективно управлять сетевыми потоками и своевременно реагировать на угрозы.

## Литература

1. Zhao X., Wu Q. Subspace-Based Anomaly Detection for Large-Scale Campus Network Traffic, Journal of Applied Mathematics, Volume 2023, No. 1, 2023, pp. 1–12.

2. Zhang W., Lazaro J.P. A Survey on Network Security Traffic Analysis and Anomaly Detection Techniques, International Journal of Emerging Technology and Advanced Applications, Volume 1, No. 4, 2024, pp 1–9.

3. Gebrye H., Wang Y., Li F. Traffic Data Extraction and Labeling for Machine Learning Based Attack Detection in IoT Networks, International Journal of Machine Learning and Cybernetics, Volume 14, No. 7, 2023, pp. 1–16.

4. Adil S., Alfoudi A.S. Traffic Data Classification in SDN Network Based on Machine Learning Algorithms, Wasit Journal of Pure Sciences, Volume 3, No. 2, 2024, pp. 161–171.

5. Fan M., Gao J., He Y., Lu Y. Traffic Fingerprints for Homogeneous IoT Traffic Based on Packet Payload Transition Patterns, Electronics, Volume 13, No. 5, 2024, p. 930.

6. Salau A., Beyene M.M. Software Defined Networking Based Network Traffic Classification Using Machine Learning Techniques, Scientific Reports, Volume 14, No. 1, 2024, pp. 1–17.

7. Rekhi A., Saxena A., Sharma C., Easwar S. A Python-Based Packet Sniffer Simulation for Network Traffic Analysis, Preprint, 2023, pp. 1–9.

8. Vorabbi L., Maltoni D., Santi S. Optimizing Data Flow in Binary Neural Networks, Sensors, Volume 24, No. 15, 2024, pp. 1–15.

## References

1. Zhao X., Wu Q. Subspace-Based Anomaly Detection for Large-Scale Campus Network Traffic, Journal of Applied Mathematics, Volume 2023, No. 1, 2023, pp. 1–12.

2. Zhang W., Lazaro J.P. A Survey on Network Security Traffic Analysis and Anomaly Detection Techniques, International Journal of Emerging Technology and Advanced Applications, Volume 1, No. 4, 2024, pp 1–9.

3. Gebrye H., Wang Y., Li F. Traffic Data Extraction and Labeling for Machine Learning Based Attack Detection in IoT Networks, International Journal of Machine Learning and Cybernetics, Volume 14, No. 7, 2023, pp. 1–16.

4. Adil S., Alfoudi A.S. Traffic Data Classification in SDN Network Based on Machine Learning Algorithms, Wasit Journal of Pure Sciences, Volume 3, No. 2, 2024, pp. 161–171.

5. Fan M., Gao J., He Y., Lu Y. Traffic Fingerprints for Homogeneous IoT Traffic Based on Packet Payload Transition Patterns, Electronics, Volume 13, No. 5, 2024, p. 930.

6. Salau A., Beyene M.M. Software Defined Networking Based Network Traffic Classification Using Machine Learning Techniques, Scientific Reports, Volume 14, No. 1, 2024, pp. 1–17.

7. Rekhi A., Saxena A., Sharma C., Easwar S. A Python-Based Packet Sniffer Simulation for Network Traffic Analysis, Preprint, 2023, pp. 1–9.

8. Vorabbi L., Maltoni D., Santi S. Optimizing Data Flow in Binary Neural Networks, Sensors, Volume 24, No. 15, 2024, pp. 1–15.



**МЕДВЕДЕВ Михаил Александрович,** старший преподаватель кафедры защиты информации, Новосибирский государственный технический университет. 630073, г. Новосибирск, проспект К. Маркса, 20. E-mail: m.medvedev@corp.nstu.ru

**MEDVEDEV Mikhail Alexandrovich,** Senior lecturer of the Department of Information Security, Novosibirsk State Technical University. 630073, Novosibirsk, K. Marksa Ave., 20. E-mail: m.medvedev@corp.nstu.ru

УДК 004.056 Вестник УрФО № 2(52) / 2024, с. 54–60

**Ахмед Т. Р., Авсиевич А. В.**

DOI: 10.14529/secur240506

# *ЛОЖНАЯ И ВРЕДОНОСНАЯ ИНФОРМАЦИЯ В КОНТЕКСТЕ ИРАКСКОГО ПРАВА*

*The article discusses research on the dissemination of false and malicious information on the information expanses of the global information network "Internet" in the context of Iraqi and Islamic law and possible ways to protect the Iraqi population from misleading, confusing and distorting public opinion. The dissemination of false and malicious information poses a serious threat to the stability of the State and its security apparatus. The consequences are diverse in terms of public safety, political unpredictability, social and economic shocks. Malicious information can create a state of chaos and sow doubt in society. The enormous speed of the spread of malicious and false information, especially in the light of new media located on the Internet, makes it difficult to confront it.*

*The study concluded that it is impossible only for regulatory state bodies to effectively establish control over what is published on the Internet in modern ways that correspond to the digital development taking place in modern mass media and communication in order to limit its promotion, introduce its scale and globality without restricting freedom of speech. As a result, it is proposed to develop a recommendation service for informing and warning Internet users.*

***Keywords:*** *malicious information, false information, fake news, internet, information protection, criminal code, Islamic law.*

# *FALSE AND MALICIOUS INFORMATION IN THE CONTEXT OF IRAQI AND ISLAMIC LAW*

*В статье обсуждаются исследования о распространении ложной и вредоносной информации на информационных просторах глобальной информационной сети «Интернет» в контексте Иракского и Исламского права и возможные способы защиты населения Ирака от введения в заблуждение, запутывание и искажения общественного мнения. Распространение ложной и вредоносной информации представляет собой серьезную угрозу для стабильности государства и его аппарата безопасности. Последствия многообразны с точки зрения безопасности населения, политической непредсказуемости, социальных и экономических потрясений. Вредоносная информация способна создать состояние хаоса и посеять сомнение в обществе. Огромная скорость распространения вредоносной и ложной информации, особенно в свете новых средств массовой информации, расположенных на просторах глобальной информационной сети «Интернет», делает затруднительным противостояние ей.*

*Результаты проведенного исследования позволяют сделать вывод, что невозможно только регулятивными государственными органами эффективно с применением современных технологий наладить контроль над тем, что публикуется в сети «Интернет». Предлагается способ защиты населения разных стран от вредоносной и ложной информации, посредством разработки программного обеспечения, реализующего функцию предупредительного сервиса.*

***Ключевые слова:*** *вредоносная информация, ложная информация, фейковые новости, интернет, защита информации, уголовный кодекс, исламское право.*

**Введение**

Проблема ложной и вредоносной информации остро стоит в настоящее время. Время гибридных войн в разных частях Земли совершенствует способы доставки вредоносной и ложной информации до населения разных стран. Проблема связана с быстрой, практически моментальной скорость распространения информации в различных средствах массовой информации. Особенно в глобальной информационной сети «Интернет». Это стало заметно в последние годы. Особенно выделяется явление представления и распространения ложной и вредоносной информации, которое характеризуется высокой скоростью распространения как в средствах массовой информации, так и в сети «Интернет» и получившее название «Фейковые новости» от английского «fake news». Данное явление подлежит всестороннему изучению для выработки эффективных методов и способов защиты населения разных стран от вредоносной и ложной информации.

Важность проводимого исследования заключается в опасности широкого распространения сфабрикованных новостей в современных средствах массовой информации, особенно в социальных сетях, и быстрого распространения среди отдельных лиц без проверки их достоверности, а также злонамеренно с целью дестабилизации обстановки в обществе.

Каждая страна в борьбе с вредоносной и ложной информацией с целью защиты населения от её воздействия вырабатывает собственные способы борьбы в зависимости от политических, религиозных и национальных особенностей.

Целью данной работы является всесторонние изучение понятие «Фейковые новости» в контексте ложной и вредоносной информации и методов борьбы с ними на примере Республики Ирак.

**Определение фейковых новостей**

Согласно проведенным исследованиям Борнмутский университет (Великобритания) на саммите СМИ стран Персидского залива «Фальшивые новости» определил термин «фейковые новости» как тип связей с общественностью, который демонстрирует преувеличенную предвзятость в одних фактах и затеняет другие, будь то через традиционные средства массовой информации или через социальные сети [1].

Исходя из исследования Лахмара Набиля [2] в работе «фейковые новости в социальных сетях и их влияние на тенденции общественного мнения», фейковыми новостями можно считать любую информацию, которая часто является ложной или вводящей в заблуждение и охватывает миллионы пользователей в разных странах.

Свободная энциклопедия «Википедия» [3] трактует понятие «фейковые новости» следующим образом: 1) информационная мистификация или намеренное распространение дезинформации в социальных медиа и традиционных СМИ с целью введения в заблуждение для того, чтобы получить финансовую или политическую выгоду; 2) новость, которая полностью составлена и сфабрикована для обмана читателя с целью увеличения трафика и прибыли.

Российская компания по разработке продуктов информационной безопасности – АО «Лаборатория Касперского» [4] определяет понятие «фейковые новости» как ложную или вводящую в заблуждение информацию, выдаваемую за реальные новости.

Большая Российская энциклопедия [5] дает, по мнению авторов, наиболее полное определение фейковых новостей: «Фейковые новости (фейк-ньюс англ. fake news – фальшивые новости, фейки) это ложная или вводящая в заблуждение информация, поданная в новостном формате с целью дискредитации конкретного лица, государства, компании или группы лиц (в том числе официальных) и компаний, нанесения ущерба и/или получения прибыли». Это определение и будет использоваться авторами в дальнейших исследованиях.

**Тактика фейковых новостей**

Ложная и вредоносная информация может проявляться разными способами. Как все виды ложной и вредоносной информации, фейковые новости обладают своей тактикой введения населения разных стран в заблуждение. Проведенное исследование в работе Defining “Fake news”: a typology of scholarly definitions [6] в 2017 году по характеру применения термина «фейковые новости» показало, что для достижения цели фейковых новостей требуется несколько методов, которые основаны:

• на сарказме, в основе которого используется сатирическое изобличение, язвительная насмешка. Высшая степень иронии - преувеличение при описании текущих событий. Данный стиль описания новостей основан на развлечении аудитории. При этом имеются случаи, когда целые новостные сюжеты полностью сфабрикованы. При подаче новостей часто используются иллюстрации в саркастической манере. Данный способ направлен на деструктивную критику политических и социальных проблем. Например, выражение сарказма в сообщениях внутри паствы в Твиттере [6,7];

• на затенении, то есть в основе новости лежит задача фальсификации истины. Базируется на реальной информации с использованием её в ложном контексте. Ложная информация часто содержит факты и цитаты, которые были тщательно отобраны и их трудно обнаружить в открытом доступе. Это вводящий в заблуждение способ, с помощью которого происходит отвлечение внимания через видимость, противоречащую истине и реальности [8]. Широко применяются методы социальной инженерии [9];

• на манипулирование контентом, то есть в основе которого лежит тот или иной способ манипулирования исходным контентом, будь то информация в письменном или графическом изображении. Если информация есть, то ей можно манипулировать. В данном случае целью обмана является сам обман. Он представляет собой нереальное и вводящее в заблуждение сообщение. И в большинстве случаев мы обнаруживаем манипулирование изображениями, которое стало простым и быстрым с развитием современных графических систем [10];

• на подмене ссылок. Основой такого способа является вводящая в заблуждение неправильная ссылка, когда содержание соответствующей новости не отражает тему, заявленную в названии (в ссылке), и транслируется через печатные, электронные или аудиовизуальные средства массовой информации, а также публикуется любыми информационными средствами [11];

• на плагиаторском контенте. Практика применения данного способа заключается в распространении новостей содержащих ложную информацию под именами известных политических или творческих деятелей. Всё это реализуется путем разработки страниц или создания фейковых аккаунтов, в которых публикуются новости, подражающие стилю указанных популярных авторов. Размещаются сфабрикованные видеоклипы, которые модифицированы с использованием технологий искусственного интеллекта. Настоящие проблемы возникают, когда журналисты обнаруживают свои имена в статьях, которые они не писали [12,13];

• на фабрикации материала. В этом случае новости изначально несут ложное содержание от начала и до конца и не имеют под собой реальной основы. Такая ложная информация полностью вводит в заблуждение её потребителей и провоцирует формирование неправильной жизненной позиции и приводит в некоторых случаях к смене жизненной позиции человека [14].

Соответственно, распространение ложных новостей различных типов специальными методами преследует одну цель: запутать людей, манипулировать их мыслями для достижения своих личных целей и повлиять на как можно большее количество получателей. Благодатной почвой для пропагандистов фейковых новостей являются социальные сети. Быстрое и многократное распространения любых новостей в социальных сетях обусловлено человеческим желанием поделиться ими с другими. Использование социальных сетей привело к вирусному распространению вводящей в заблуждение и ложной информации между собеседниками. В современных социальных сетях затруднено отслеживание фейковых новостей из-за массового распространения потока разнородной информации.

Вредоносность социальных сетей исследуется в арабском мире в разных разрезах, о чём говорят работы [10-15]. Ложная и вредоносная информация приносит любому государству в мире большой вред в сфере безопасности [16], социальной сфере и наносит непоправимый вред экономике. Поэтому в разных государствах имеются свои законы, например, законодательный механизм распространения информации в сети Интернет [16] или Правовое регулирование информационной безопасности в условиях цифровизации и трансформации права [17] в Российской Федерации. Основываясь на национальных интересах, Иракский законодатель разработал правовые положения для тех, кто пропагандирует и распространяет ложную и вредоносную информацию.

Например, статья (179) Уголовного кодекса Ирака предусматривает наказание для тех, кто намеренно распространяет ложные или тенденциозные новости, данные или слухи во время войны или намеревается распространять подстрекательскую пропаганду, если это может нанести ущерб военным приготовлениям к защите страны или военным действиям вооруженных сил либо вызвать панику. За распространение ложных слухов внутри страны наказание регулируется статьёй (180) УК Ирака, которая предусматривает наказание для любого гражданина, умышленно передающего за границу ложные или тенденциозные новости, данные или слухи о внутренних делах государства. Также Иракский законодатель не оставил без внимания ложные новости и слухи, которые распространяются в мирное время. В Уголовном кодексе в статье 210 предусматривается наказание для тех, кто умышленно распространяет ложные новости, заявления или слухи и нарушает общественную безопасность, сеет террор среди людей или наносит вред обществу. Для тех, кто распространяет ложные новости и слухи любым публичным способом, предусмотрена статья (211) за ложные новости или сфабрикованные документы, которые могут вызвать волнение общественной безопасности или нанести ущерб общественным интересам.

Хорошо рассмотрены аспекты Иракского законодательства авторами в работах [17-23], которые полностью характеризуют отношение Иракского права к ложной и вредоносной информации.

**Обсуждение**

В результате проведенного исследования возникли вопросы:

1) Как обеспечить информационную безопасность граждан страны?

2) Как информировать граждан о возможном наличии ложной и вредоносной информации в просматриваемой ими информации в контенте или в социальных сетях?

В настоящее время, несмотря на широкое изучение проблемы фейковых новостей в научной среде, разработку и принятие подзаконных и законных актов, регламентирующих понятие фейковых новостей, введение адми-

нистративной и уголовной ответственности за распространение ложной и вредоносной информации, мер по обеспечению информационной безопасности граждан недостаточно. Не все могут распознать ложный и вредоносный характер информации, и многие не понимают, почему несут наказания. В этой связи разработка предупредительного сервиса для пользователей сети «Интернет» об опасном контенте, имеющим признаки ложной и вредоносной информации, является актуальной задачей.

Предупредительный сервис является надстройкой для браузера (плагина) или дополнительной программы, которая будет контролировать трафик интеллектуальными методами оценки информации, например, с помощью нейросетевых алгоритмов, и выдавать предупреждение или вероятностную оценку о наличии в просматриваемых материала ложной или вредоносной информации. Вопрос о доверии к данной информации остается на усмотрение пользователя.

**Заключение**

В работе проанализированы и всесторонне изучены различные виды фейковых новостей в контексте распространения ложной и вредоносной информации. Исследовано разрушительное воздействие такой информации на безопасность государства, его экономическое и социальное благополучие, а также на жизнь граждан.

Изучены законодательные меры, предпринимаемые Республикой Ирак для борьбы с фейковыми новостями в информационном пространстве.

На основе проведенного в работе анализа предлагается способ обеспечения информационной безопасности граждан. Способ предполагает разработку программного обеспечения (плагина для веб браузера) реализующего функцию предупредительного сервиса, заключающегося в предупреждении пользователей сети «Интернет» об опасном контенте, имеющим признаки фейковых новостей.

**Литература**


1. Sanaa, Gulf Summit Media Fake News, Report of the Doha Center for Media Freedom, Qatar, 2017, p 20.

2. Lahmar Nabil, "Fake news via social media networks and its effects on public opinion trends", Al-Baheth Academic Journal, Volume 7, Issue 02, 2020.

3. Википедия: сайт. Свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/Фальшивые новости (дата обращения: 19.06.2024).

4. Как распознать фейковые новости// Kaspersky. Сайт. URL: https://www.kaspersky.ru/resource-center/preemptive-safety/how-to-identify-fake-ews?ysclid=lv2nxd87su567158669 (дата обращения: 03.07.2024).

5. Фейковые новости // Большая энциклопедия. Сайт. URL: https://bigenc.ru/c/feikovye-novosti-3c3315?ysclid=lv2oqobuit18469325 (дата обращения: 015.05.2024).

6. Tandoc, E. C., Jr., Lim, Z. W., & Ling, R. (2018). Defining "fake news": a typology of scholarly definitions. Digital Journalism, 6(2), pp. 137-153. doi:10.1080/21670811.2017.1360143.

7. Abu Arqoub Omar, "Fake news tweeting within the flock", Journal of Journalism, Issue 13, 2019.

8. Claude Younan, "Verbal misleading and mechanisms of controlling opinion", Dar Al-Nahda Al-Arabiya, Cairo, 2010, p. 14

9. Халилаева Э.И., Маслова М.А., Герасимов В.М. система противодействия методам социальной инженерии в области информационной безопасности// Вестник УрФО No 2(48) / 2023, с. 54–61.

10. Mufdi Al-Shammari Ahmed Mahmoud, "Kuwaiti journalists' reliance on Twitter as a source of information on corruption issues", PhD thesis, Yarmouk University, 2017, p. 17.

11. Al-Dailami Abdul-Razzaq, "Problems of fabricated news and its impact on shaping public opinion", Media Studies, Al-Jazeera Center for Studies, Qatar, 2018.

12. Abdul Hadi Sabrina, "The impact of the characteristics of social networking sites on the different values of young people", Al-Balqa Applied University, p. 13. 2019

13. Bukhari Malika, "False news via social networking sites in the events of the Yellow Vests protests in France", Journal of Media Studies. Issue 9, p. 15. 2019.

14. Bin Mazhar Saleh Al-Shammari Ismail, "Rumor in the Arab Electronic Press and its Impact on Society", University of Sudan 2017, p. 7.

15. Abbas Abdul Aziz, "Rumor and its Effects on the Individual and Society", Scientific Researcher Magazine, Volume 08, Issue 20, p. 7. 2019.

16. Ахмед, Т. Р. Вредоносная информация в сети интернет и борьба с ней / Т. Р. Ахмед, А. В. Авсиевич // Достижения науки и технологий, культурные инициативы и устойчивое развитие - ДНиТ-III-2024: сборник научных статей по материалам III Всероссийской научной конференции с международным участием, Красноярск, 01–02 марта 2024 года. – Красноярск: Общественное учреждение "Красноярский краевой Дом науки и техники Российского союза научных и инженерных общественных объединений", 2024. – С. 80-84. – DOI 10.47813/dnit-III.2024.11.3002.

17. Добкач Л. Я., Тарапанова Е. А. Законодательный механизм ограничения распространения информации в сети интернет\\ Вестник УрФО № 2(32) / 2019, С. 30–38. DOI: 10.14529/secur190205

18. Полякова Т. А., Минбалеев А. В., Бойченко И. С. Концептуальные подходы к правовому регулированию информационной безопасности в условиях цифровизации и трансформации права// Вестник УрФО № 3(33) / 2019, С. 64–68. DOI: 10.14529/secur190307

19. Abdel Hamid Al-Shawarby, "Expressive Crimes, Crimes of the Press and Publishing", Dar Al-Kutub and Arab Studies, Alexandria, p. 19, 2018.

20. Mohamed Zaki Abu Amer, "Principles of Criminology and Punishment", Dar Al-Jamiah for Publishing, Alexandria, p. 24, 1992.

21. Abdel Hamid Al-Shawarbi, "Expressive Crimes, Crimes of the Press and Publishing", Dar Al-Kutub and Al-Dirasat Al-Arabiya, Alexandria, 2018, p. 19.

22. Hassoun Obaid Hajij and Hassan Khanjar Ajeel, "The Personality of Original Penalties, a Comparative Study", a research published in Al-Muhaqqiq Al-Hilli Journal for Legal and Political Sciences, Issue Two, Year Six, p. 23. 2014.

23. Salem Rawdan Al-Moussawi, "The Terrorist Crime", published in the Judicial Bulletin, Issue No. 1. 2015.

## References

1. Sanaa, Gulf Summit Media Fake News, Report of the Doha Center for Media Freedom, Qatar, 2017, p 20.

2. Lahmar Nabil, "Fake news via social media networks and its effects on public opinion trends", Al-Baheth Academic Journal, Volume 7, Issue 02, 2020.

3. Vikipediya: sajt. Svobodnaya enciklopediya. URL: https://ru.wikipedia.org/wiki/Fal'shivye novosti (data obrashcheniya: 19.06.2024).

4. Kak raspoznat' fejkovye novosti// Kaspersky. Sajt. URL: https://www.kaspersky.ru/resource-center/preemptive-safety/how-to-identify-fake-ews?ysclid=lv2nxd87su567158669 (data obrashcheniya: 03.07.2024).

5. Fejkovye novosti // Bol'shaya enciklopediya. Sajt. URL: https://bigenc.ru/c/feikovye-novosti-3c3315 ?ysclid=lv2oqobuit18469325 (data obrashcheniya: 015.05.2024).

6. Tandoc, E. C., Jr., Lim, Z. W., & Ling, R. (2018). Defining "fake news": a typology of scholarly definitions. Digital Journalism, 6(2), pp. 137-153. doi:10.1080/21670811.2017.1360143.

7. Abu Arqoub Omar, "Fake news tweeting within the flock", Journal of Journalism, Issue 13, 2019.

8. Claude Younan, "Verbal misleading and mechanisms of controlling opinion", Dar Al-Nahda Al-Arabiya, Cairo, 2010, p. 14

9. Halilaeva E.I., Maslova M.A., Gerasimov V.M. sistema protivodejstviya metodam social'noj inzhenerii v oblasti informacionnoj bezopasnosti// Vestnik UrFO No 2(48) / 2023, s. 54–61.

10. Mufdi Al-Shammari Ahmed Mahmoud, "Kuwaiti journalists' reliance on Twitter as a source of information on corruption issues", PhD thesis, Yarmouk University, 2017, p. 17.

11. Al-Dailami Abdul-Razzaq, "Problems of fabricated news and its impact on shaping public opinion", Media Studies, Al-Jazeera Center for Studies, Qatar, 2018.

12. Abdul Hadi Sabrina, "The impact of the characteristics of social networking sites on the different values of young people", Al-Balqa Applied University, p. 13. 2019

13. Bukhari Malika, "False news via social networking sites in the events of the Yellow Vests protests in France", Journal of Media Studies. Issue 9, p. 15. 2019.

14. Bin Mazhar Saleh Al-Shammari Ismail, "Rumor in the Arab Electronic Press and its Impact on Society", University of Sudan 2017, p. 7.

15. Abbas Abdul Aziz, "Rumor and its Effects on the Individual and Society", Scientific Researcher Magazine, Volume 08, Issue 20, p. 7. 2019.

16. Ahmed, T. R. Vredonosnaya informaciya v seti internet i bor'ba s nej / T. R. Ahmed, A. V. Avsievich // Dostizheniya nauki i tekhnologij, kul'turnye iniciativy i ustojchivoe razvitie - DNiT-III-2024: sbornik nauchnyh statej po materialam III Vserossijskoj nauchnoj konferencii s mezhdunarodnym uchastiem, Krasnoyarsk, 01–02 marta 2024 goda. – Krasnoyarsk: Obshchestvennoe uchrezhdenie \"Krasnoyarskij kraevoj Dom nauki i tekhniki Rossijskogo soyuza nauchnyh i inzhenernyh obshchestvennyh ob"edinenij\", 2024. – S. 80-84. – DOI 10.47813/dnit-III.2024.11.3002.

17. Dobkach L. Ya., Tarapanova E. A. Zakonodatel'nyj mekhanizm ogranicheniya rasprostraneniya informacii v seti internet\\\\ Vestnik UrFO № 2(32) / 2019, S. 30–38. DOI: 10.14529/secur190205

18. Polyakova T. A., Minbaleev A. V., Bojchenko I. S. Konceptual'nye podhody k pravovomu regulirovaniyu informacionnoj bezopasnosti v usloviyah cifrovizacii i transformacii prava// Vestnik UrFO № 3(33) / 2019, S. 64–68. DOI: 10.14529/secur190307

19. Abdel Hamid Al-Shawarby, "Expressive Crimes, Crimes of the Press and Publishing", Dar Al-Kutub and Arab Studies, Alexandria, p. 19, 2018.

20. Mohamed Zaki Abu Amer, "Principles of Criminology and Punishment", Dar Al-Jamiah for Publishing, Alexandria, p. 24, 1992.

21. 21. Abdel Hamid Al-Shawarbi, "Expressive Crimes, Crimes of the Press and Publishing", Dar Al-Kutub and Al-Dirasat Al-Arabiya, Alexandria, 2018, p. 19.

22. Hassoun Obaid Hajij and Hassan Khanjar Ajeel, "The Personality of Original Penalties, a Comparative Study", a research published in Al-Muhaqqiq Al-Hilli Journal for Legal and Political Sciences, Issue Two, Year Six, p. 23. 2014.

23. Salem Rawdan Al-Moussawi, "The Terrorist Crime", published in the Judicial Bulletin, Issue No. 1. 2015.

---

**АСИЕВИЧ Александр Викторович,** кандидат технических наук, доцент федерального бюджетного государственного образовательного учреждения высшего образования «Самарский государственный технический университет». 443100, г. Самара, ул. Молодогвардейская, 244.; доцент федерального государственного бюджетного образовательного учреждения высшего образования «Самарский государственный медицинский университет» Министерства здравоохранения Российской Федерации. 443099, г. Самара, ул. Чапаевская, 89. E-mail: a.v.avsievich@samsmu.ru

**АХМЕД Тамер Рашид,** аспирант федерального бюджетного государственного образовательного учреждения высшего образования «Самарский государственный технический университет». 443100, г. Самара, ул. Молодогвардейская, 244. E-mail: thameer987@gmail.com

**AVSIEVICH Alexander Viktorovich,** Candidate of Technical Sciences, Associate Professor Federal Budgetary State Educational Institution of Higher Education "Samara State Technical University". 443100, Samara, Molodogvardeyskaya str., 244.; associate Professor of the Federal State Budgetary Educational Institution of Higher Education "Samara State Medical University" of the Ministry of Health of the Russian Federation. 443099, Samara, Chapaevskaya str., 89. E-mail: a.v.avsievich@samsmu.ru

**AHMED Tamer Rashid,** postgraduate student of the Federal budgetary State Educational Institution of Higher Education "Samara State Technical University". 443100, Samara, Molodogvardeyskaya str., 244. E-mail: thameer987@gmail.com

УДК 004.942:519.23/.25 Вестник УрФО № 3(53) / 2024, с. 61–72

**Жукова М. Н., Яковлева А. О.** DOI: 10.14529/secur240307

# *РАЗРАБОТКА РЕШЕНИЯ ДЛЯ ПРОВЕДЕНИЯ GAP АНАЛИЗА И ПРИВЕДЕНИЯ В СООТВЕТСТВИЕ УРОВНЮ ЗАЩИЩЕННОСТИ ПРИ ПРОВЕДЕНИИ ОЦЕНКИ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ ПО ЗАЩИТЕ ИНФОРМАЦИИ ДЛЯ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ*

*В статье представлена проблема оценки соответствия кредитно-финансовой организации требованиям по защите информации в соответствии с ГОСТ 57580.2-2018. Рассматриваются и анализируются показатели оценки, значение основных метрик и расчетных величин. Представлены требования к процессу проведения оценки соответствия, описаны показатели и требования к их значениям и расчету в соответствии с ГОСТ Р 57580.2-2018.*

*Описаны основные подходы, применяемые для проведения оценочных процедур. Показаны основные трудности, связанные со сложностью однозначного соответствия результатов аудита и GAP анализа, проводимого финансовой организацией в рамках предварительных процедур оценки соответствия требованиям по защите информации. Выявлены основные проблемы, представлен подход, позволяющий в рамках единой оценочной процедуры совместить расчет оценки, подбор параметров и решить задачу оптимизации при подборе средств защиты информации. Представлены обобщенные схемы программного решения по автоматизации процедуры определения базовых мер и оценки соответствия по ГОСТ 57580.1 и 57580.2. Описан алгоритм расчета оценки, позволяющий получить численные значения для каждого контура безопасности, входящего в состав целевой информационной системы финансовой организации.*

***Ключевые слова:*** *оценка соответствия, кредитно-финансовые организации, защита информации, метрики.*

# DEVELOPMENT OF A SOLUTION FOR CONDUCTING GAP ANALYSIS AND ADJUSTING THE LEVEL OF SECURITY WHEN ASSESSING COMPLIANCE WITH INFORMATION SECURITY REQUIREMENTS FOR FINANCIAL INSTITUTIONS

*The article presents the problem of assessing the compliance of a credit and financial institution with the requirements for information security in accordance with GOST 57580.2-2018. The assessment indicators, the meaning of the main metrics and calculated values are considered and analyzed. The requirements for the conformity assessment process are presented, the indicators and requirements for their values and calculation in accordance with GOST R 57580.2-2018 are described. The main approaches used to carry out assessment procedures are described. The main difficulties associated with the complexity of unambiguous correspondence between the audit results and the GAP analysis carried out by a financial institution within the framework of preliminary procedures for assessing compliance with information security requirements are shown. The main problems are identified, an approach is presented that allows, within the framework of a single assessment procedure, to combine the assessment calculation, the selection of parameters and solve the optimization problem when selecting information security tools. Generalized schemes of a software solution for automating the procedure for determining basic measures and assessing compliance in accordance with GOST 57580.1 and 57580.2 are presented. An algorithm for calculating an assessment is described, which allows obtaining numerical values for each security contour included in the target information system of a financial organization.*

***Keywords:*** *conformity assessment, financial institutions, information security system, metrics.*

**Введение**

В организациях финансовой сферы вопросам информационной безопасности уделяется большое внимание, поскольку результатом нарушения работы составляющих их систем и сервисов, посредством реализации угроз, может быть прямой ущерб интересам собственников и клиентов. Для противостояния таким угрозам и обеспечения эффективности мероприятий по ликвидации неблагоприятных последствий инцидентов ИБ (их влияния на операционный, репутационный, стратегический и иные риски) в организациях БС РФ следует обеспечить достаточный уровень ИБ [1].

Оценка ситуации в сфере инцидентов информационной безопасности, происходящих с финансовыми системами, показывает два основных направления: использование методов социальной инженерии для осуществления мошеннических действий с денежными средствами клиентов банковских систем, а также атаки на техническую сторону инфраструктуры банковских систем [2]. Таким обра-

зом, требуется обеспечение необходимого уровня защиты информации для финансовых организаций. Под финансовыми организациями принято понимать все организации, которые предоставляют финансовые услуги и должны получить разрешение Банка России о допуске на финансовый рынок. В зависимости от вида организации это может быть, как лицензия, так и включение сведений в реестр или аккредитация [3].

**Подход Банка России к обеспечению безопасности финансовых систем**

Инфраструктура крупной финансовой системы является сложной и многогранной, так как речь идет об особо выделяемой клиентской части, о целевой системе в которой происходит основная обработка информации по всем транзакциям и обязательном взаимодействии с базами данных и другими видами хранилищ информации, о защищаемых каналах передачи информации, процессинговом центре и тд. Требуется особый подход к формированию требований по защите информации, рассмотрению защищенности целевой системы, ее оценке и требованиях к оценочным мероприятиям [4]. История действий Банка России в части разработки нормативно-методических документов по обеспечению информационной безопасности финансовых систем имеет множество этапов — разработка и утверждение СТО ИБ ИББС, множества сопутствующих и дополняющих различные практические аспекты положений. На сегодняшний день система документов переведена в систему стандартов ГОСТ 57580.X, посвященных циклу GAP анализа, аудита защищенности финансовых систем, определению базовых мер по защите информации, оценочных процедур [5].

Основные характеристики документов приведены ниже:

1) ГОСТ Р 57580.1 – 2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер» - устанавливает защитные меры, организационные и технические, и уровни защиты информации для финансовых организаций, таких как кредитные организации, некредитные финансовые организации РФ, а также субъекты национальной платежной системы [6].

Стандарт выделяет 8 процессов и 10 подпроцессов, для которых разработаны меры защиты информации, применяемые к различным объектам информатизации, в том числе АС, которые используются для построения эффективной модели бизнес-процесса и технологического процесса, непосредственно связанных с предоставлением организацией финансовых услуг.

2) ГОСТ Р 57580.2 – 2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия» – используется чтобы определить, насколько организация соответствует требованиям ГОСТ Р 57580.1, который описывает методологию проведения оценки выбора и реализации финансовой организацией организационных и технических мер защиты информации [7].

Схематично процессы, к которым применяются меры защиты информации, и план их оценки в соответствии с ГОСТами изображены на рисунке ниже (рисунок 1).

Проведение оценки соответствия, согласно требованиям, должно проводиться независимой организацией, обладающей необходимым уровнем компетенции и имеющей лицензию ФСТЭК на деятельность по технической защите конфиденциальной информации [7].

3) ГОСТ Р 57580.3-2022 «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения» [8]. Данный стандарт устанавливает требования к составу и содержанию мер по управлению риском реализации информационных угроз для уровней защиты, которые применяются финансовыми организациями в рамках планирования, реализации, контроля и совершенствования системы управления таким риском.

4) ГОСТ Р 57580.4-2022 «Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Базовый состав организационных и технических мер» [9]. Устанавливает требования к составу и содержанию мер обеспечения операционной надежности для тех уровней защиты, которые применяют финансовые организации при определении базового состава таких мер. В ГОСТе отражены 3 уровня защиты (минимальный, стандартный, усиленный) в соответствии с нормативными актами Банка России, которые зависят от вида деятельности, объема операций, размера и значимости организации для финансовой системы.


Рис. 1. Взаимосвязь стандартов

В целом архитектуру рассмотренных документов можно представить в следующем виде (рисунок 2).

На данный момент отсутствуют документы, определяющие методику оценки зрелости ГОСТ Р 57580.3-2022 и методику оценки соответствия ГОСТ Р 57580.4-2022. И определенное время эти документы не были утверждены к обязательному исполнению положениями Банка России, но рекомендованы финансовым организациям для изучения и начала работы по возможной перестройке СОИБ для будущего соответствия стандартам.

Однако, 27 марта 2024 года на сайте Банка России опубликован документ №7-МР от 21.03.2024 «Методические рекомендации по управлению риском информационной безопасности и обеспечению операционной надежности» [10] для использования кредитными и некредитными финансовыми организациями. Несмотря на то, что стандарты с методиками оценок ГОСТ Р 57580.3-2022 и ГОСТ Р 57580.4-2022 еще не выпущены, Банк России рекомендует уже сейчас готовиться к внедрению требований этих стандартов.

Требования по базовым мерам защиты информации, а также оценка соответствия (это ГОСТ 57580.1 и 57580.2) — внедрены начиная с 2018 года и работа по ним уже проведена. По оценке рисков информационной


Рис. 2. Архитектура стандартов серии 57580.X

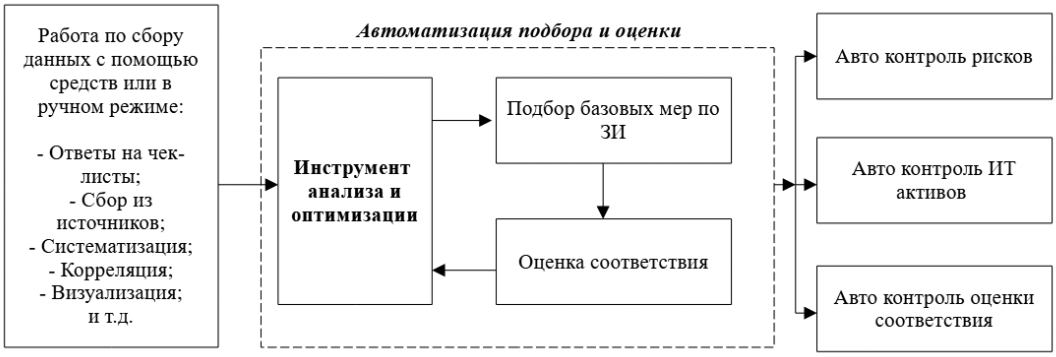


Рис. 3. Общая схема подхода к автоматизации процедур GAP-анализа

безопасности и оценке операционного риска (это ГОСТ 57580.3 и 57580.4) для всех кредитных организаций срок внедрения требований объединен и зависит от размера активов:

- если размер активов составляет 500 млрд. рублей и более - до 31 декабря 2025;

- всем остальным кредитным организациям внедрение этих стандартов рекомендовано завершить до 31 декабря 2026 года.

Практика показала, что работа с вышеуказанными ГОСТами – процесс сложный, требующий от организации большого количества временных, трудовых и финансовых затрат. Сложность заключается в том, чтобы верно истолковать, корректно и в соответствующие сроки выполнить предписанные требования. Это подтверждается наличием огромного числа вопросов, задаваемых регулятору. Например, на сайте сообщества Ассоциации банков России, объединяющего коммерческие банки и другие кредитные организации, в новостях нередко упоминаются пояснения и ответы на вопросы по исполнению требований к защите информации, задаваемые ЦБ, как основному регулятору [11].

## Автоматизация и контроль требований по обеспечению защищенности финансовых системам

При выполнении требований регулятора организация может столкнуться с классической проблемой периодичности контроля, когда между аудитами (особенно актуально для организаций, где постоянно происходят изменения) возможно серьезное изменение в инфраструктуре и процессах.

При отсутствии отлаженного постоянного процесса управления соответствием, при очередном аудите может выясниться, что нужна доработка систем и внедрение мер. Не говоря о том, что проблема с реализацией мер может привести к фактической реализации самих рисков информационной безопасности и прямым потерям.

Согласно информации Positive Technologies, количество успешных кибератак в финансовом секторе год от года растет: в третьем квартале 2023 года было зафиксировано вдвое больше уникальных киберинцидентов, чем в аналогичном периоде годом ранее, что говорит о пристальном внимании преступников к отрасли [2]. Это же подтверждает и ЦБ, показывая прирост объема похищенных финансовых средств почти на 30% [12].

Очевидно, что возникает потребность в автоматизации Compliance процессов в целях постоянного контроля защищенности систем участниками кредитно-финансовой сферы. Внедрение соответствующих решений по автоматизации решит проблему постоянного контроля рисков ИБ и соответствия требованиям, упростит и удешевит прохождение аудитов, поможет правильно расставлять приоритеты при реагировании на проблемы [13].

Такое решение может принести не только экономическую выгоду (сокращение серьезной статьи расходов на предварительный аудит), но и принести практическую пользу — в виде определенной помощи при принятии решений о наборе тех или иных средств защиты информации и проведении дальнейшей автоматической оценки соответствия в связи с изменениями в инфраструктуре целевой информационной системы. Общее представление о разрабатываемом подходе можно представить в следующем виде (рисунок 3).

Одной из проблем является отсутствие алгоритма действий, применяя который можно было бы выстроить в организации соответствующую критериям и требованиям и

при этом результативную систему защиты ИБ. Об этом свидетельствует вопрос Ассоциации банков России №25 из письма с вопросами по выполнению требований ГОСТ Р 57580.1 – 2017 и 57580.2 – 2018: «Планируется ли организовать разработку методички по применению ГОСТ Р 57580.2 и критериям принятия решений по оценке мер ЗИ ГОСТ Р 57580.1 для обеспечения сходных и повторяемых результатов оценки соответствия?» [11].

На сегодняшний день задача оценки соответствия решается двумя разными способами:

1) используя внутренние силы организации: самостоятельная работа по выбору мер, с учетом их применимости, и способов их реализации, а затем проведение оценки соответствия внешней организацией;

2) передача на аутсорсинг: привлечение сторонних специалистов для приведения системы к нужному уровню оценки.

Анализ первого подхода показал, что есть сложности с реализацией требований организациями самостоятельно, которые описываются как внутренними специалистами по ИБ финансовых организаций на различных вебинарах и форумах, так и различными компаниями, предлагающими передать заботы по проведению мероприятий в рамках ГОСТ Р 57580.1 – 2017 и ГОСТ Р 57580.2 – 2018 на аутсорсинг для получения высоких оценок соответствия:

• проблемы перехода с СТО БР ИББС-1.0 – 2014 на ГОСТ Р 57580.1 – 2017 по причине увеличения количества новых требований, которых не было ранее, что, соответственно, приводит к получению низких оценок;

• высокая трудоемкость проведения оценки риска информационной безопасности – определение всех информационных активов, угроз и критичности последствий реализации риска ИБ, сложности дальнейшего использования полученных результатов для оценки остаточного операционного риска, вызванного неполным или некачественным выбором и применением организационных и технических мер защиты информации;

• большой объём работы – выявление всех бизнес и технологических процессов предоставления финансовых услуг, их составляющих и характеристик, после чего определение совокупности объектов информатизации с единой степенью критичности, в отношении которых должен применяться единый перечень мер защиты информации – контуров безопасности;

• необходимость наличия опытных и компетентных аудиторов, специалистов в связи со сложностью аудита требований ЦБ в части управления рисками и операционной надежностью.

Постоянные изменения законодательства и проверки ЦБ РФ сильно затрудняют контроль соответствия актуальным требованиям, а аудиты часто заканчиваются неудовлетворительной оценкой [14]. При этом, начиная с 2023 года большинству организаций требуется иметь оценку соответствия не ниже 4 уровня – 85%. Этот показатель является довольно высоким, причем его достижение, зачастую, требуется в кратчайшие сроки — это требует кадровых и финансовых ресурсов компании, количество которых всегда ограничено [15].

Таким образом, очевидным преимуществом должен обладать второй подход — привлечение сторонних компаний, обладающих профессиональными компетенциями. Работа внешних компаний строится по практически одинаковому сценарию:

1) сбор информации и обследование IT-инфраструктуры;

2) предварительная оценка (GAP-анализ), на котором проводят предварительную оценку, из которой становится известным список проблемных областей и областей для улучшения;

3) устранение недостатков, разработка внутренней нормативной документации (ВНД), внедрение средств защиты информации (СЗИ);

4) итоговая оценка, целью которой является оценка эффективности проработки проблемных областей и анализ полученных результатов;

5) формирование отчета по требованиям регулятора и согласование совместно с заказчиком [13].

Интересным является характеристика подходов к повышению оценки по затратам и возможным приростам показателей оценки, представленным в таблице 1.

Анализ результатов применения второго подхода — привлечения сторонних компаний на оценку и формированию мер по защите информации, показывает, что, как правило, все сводится к реализации набора наиболее выгодных, имеющих наибольший вклад в получение итогового показателя, решений. Например, реализация технической меры с использованием облачного решения для повы-

*Таблица 1.*

**Характеристики подходов повышения оценки**

(BI.ZONE «Как повысить оценку ГОСТ 57580: быстро, эффективно, с первого раза» [15])

| Подход | Размер бюджета* | Срок проекта | Повышение оценки |
|---|---|---|---|
| Разработка ОРД | Малый | 1-2 мес. | 0,16 |
| Разработка ОРД и полное внедрение процесса | Средний | 3-5 мес. | 0,57 |
| Подключение сервисов кибербезопасности, внедрение СЗИ | Большой | 2-6 мес. | 0,37 |

шения итоговой оценки, поскольку такой способ позволяет существенно и в короткие сроки достичь результата. Однако дальнейшая судьба реализованных, таким способом, процессов информационной безопасности финансовой организации остается неизвестной. Процедура оценки соответствия – процедура периодическая и очень сложно гарантировать, что подключенные сервисы, повышающие оценку, останутся функционировать и после ее проведения. В любом случае, обеспечение их дальнейшего сопровождения является затратным с финансовой точки зрения.

Рассмотрение существующих подходов, а также задачи автоматизации и контроля соответствия требованиям нормативных документов Банка России в области обеспечения информационной безопасности показывают наличие определенных проблем:

1) отсутствие подхода к анализу соответствия результатов аудита и применяемых оценочных процедур в рамках GAP анализа;

2) необходимость применения или разработки алгоритмов оптимизации для подбора и оценки эффекта от внедрения тех или иных мер по защите информации, в соответствии с требованиями ГОСТ 57580.1

3) необходимость разработки модели анализа и оценки применимости информации из целевой информационной системы для формирования дополнительных сведений при процедуре аудита и оценки финансовой системы.

### Разработка решения по анализу соответствия результатов аудита и применяемых оценочных процедур в рамках GAP анализа для кредитно-финансовой сферы

В большинстве случаев сложности возникают из-за несоответствия результатов оценки, либо из-за неоднозначности трактовки реализованных мер по защите информации различными аудиторскими компаниями. Это может зависеть от квалификации специалистов, от того набора мер, которые они привыкли «видеть» в других финансовых системах и еще от целого спектра других причин. Конечно, данные разногласия в оценке не будут прямо противоположными по оценке (0 или 1), но в данном случае речь может идти о достаточно серьезных изменениях в общей оценке (когда по 0,5 ставится по нескольким мерам в разных подпроцессах и это имеет накопительный эффект).

Требуется подход, позволяющий работать с требованиями и принимать решения по обеспечению защиты финансовых организаций, причем, как самостоятельно при реализации проекта, так и используя его в качестве механизма контроля действий внешних специалистов. В общем виде основные этапы такого решения представлены на рисунке 4.

Последовательность действий, представленная на схеме, выглядит следующим образом:

1) сведения об имеющейся системе защиты финансовой организации загружаются специалистом в базовый модуль, который представляет собой «калькулятор», позволяющий вычислить оценку уровня защиты на текущий момент;

2) по результатам работы базового модуля выводятся результаты аудита, которые содержат информацию о параметрах, имеющих низкую оценку (потенциальные места доработки), в форме базового отчета, который можно сразу отдать лицу, принимающему решение (ЛПР) и на этом закончить работу, а можно загрузить в модуль подбора;

3) в модуле подбора возможны следующие сценарии: потенциальные места доработки, полученные в модуле результатов аудита, можно сравнить со списком решений,

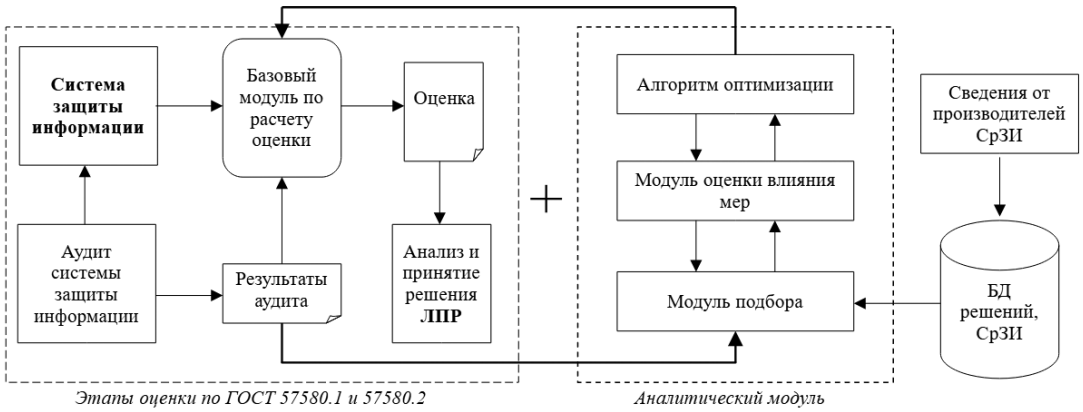


Рис. 4. Общая схема решения по анализу соответствия результатов аудита и применяемых оценочных процедур в рамках GAP анализа

предлагаемых производителями, которые закрывают те или иные требования и результаты этой работы в виде предложений отдать ЛПР, либо загрузить полученную информацию в аналитический модуль;

4) в аналитическом модуле в отличие от простого сравнения списков минусов и решений выполняется анализ возможностей дополнительной настройки существующих средств и систем в организации, а также оптимизированный подбор решений в зависимости от их стоимости или количества возможного закрытия недоработанных мест (максимальный охват закрытия требований), а уже затем передача этой информации ЛПР.

Разрабатывается программное решение для расчета базовых мер по требованиям ГОСТ 57580.1. Это решение реализовано в виде «калькулятора» для подбора необходимых базовых мер, чтобы лица, принимающие решение о внесении изменений в систему защиты информации, могли получить сводную информацию об уровне соответствия требуемому уровню защищенности, определенному для контура (контуров) безопасности соответствующими нормативно-правовыми актами.

В результате работы первого блока решения должен быть выполнен подбор базовых мер и проведения их предварительная оценка.

Для каждого контура безопасности проводится расчет оценки Ei, более подробно процедура расчета представлена на рисунке 5. Расчет оценки является одним из внутренних модулей, результат выполнения которого дает требуемый минимальный уровень оценки и определяет минимально необходимый набор базовых мер.

Таким образом, в результате работы первого модуля программного средства будет получен автоматизированный процесс оценки внесения изменений в целевую информационную систему и получен, соответствующий требованиям ГОСТ 57580.1, набор базовых мер по защите информации. Все меры рассчитаны в соответствии с требованиями ГОСТ 57580.2 по оценке соответствия базовых мер необходимому уровню показателя защищенности финансовой системы.

**Заключение**

Обеспечение защищенности финансовых систем сложная и трудоемкая задача. Это касается не только практической реализации защитных мер, внедрения и установки разнообразных средств защиты информации. Но и разработки методологических основ по формированию единого базиса, который мог бы охватывать и практические средства, и оценку рисков, в том числе операционных, а также унифицировать подходы к общей оценке соответствия финансовых систем требованиям по обеспечению информационной безопасности [16].

Банк России, как главный регулятор в кредитно-финансовой сфере, со своей стороны прикладывает максимальные усилия в сфере разработки методологических основ, их пересмотру и соответствию современным тенденциям, выпуску положений по различным практическим аспектам обеспечения защищенности тех или иных сегментов финансовой информационной системы. Выпущенная серия ГОСТ 57580.X призвана упорядочить процессы формирования защитных мер и последующей оценки соответствия требо-

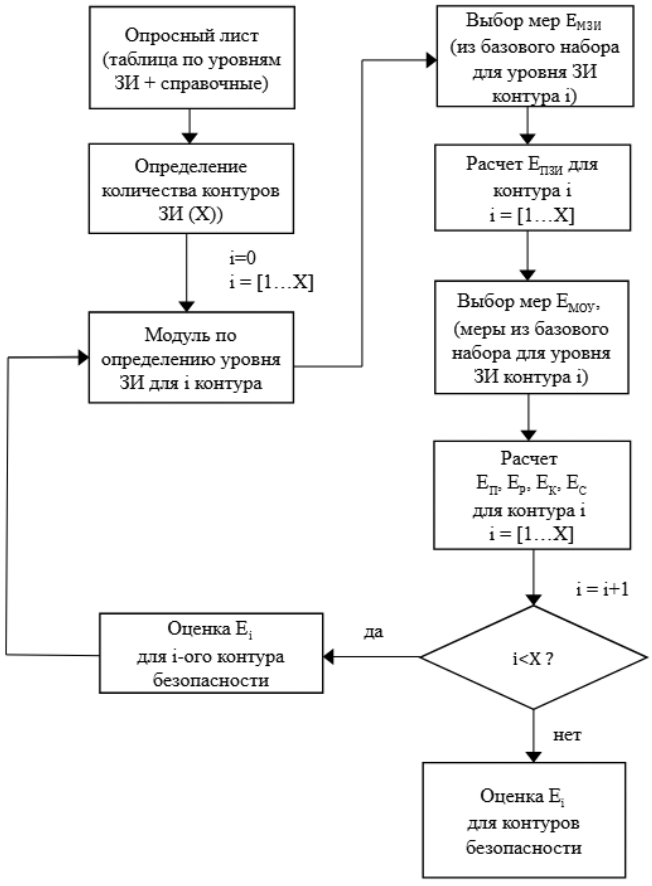


Рис. 5. Алгоритм расчета оценки Ei для каждого контура безопасности

ваниям по защите информации. Внедрение требований ГОСТ показывает достаточно хорошие практические результаты и позволяет пользоваться единой системой оценки соответствия.

Однако, часть оценочных процедур имеет неоднозначность при сопоставлении результатов внутреннего GAP анализа и последующего аудита сторонней компанией. Это может (и приводит) к серьезным разногласиям по оценке внедренных защитных мер, финансовым и репутационным потерям, существенному объему последующих работ по устранению разногласий (или выполнению рекомендаций аудитора). Пропустить этап предварительного GAP анализа со стороны финансовой компании также будет являться ошибочным — чаще всего это приведет к неготовности организации проходить процедуру оценки соответствия требованиям по защите информации.

Таким образом, требуется решение, снимающее неоднозначность оценки после прохождения аудита и результатов GAP анализа. Данное решение должно полностью выполнять требования ГОСТ 57580.1 и 57580.2 и в то же время обладать внутренним механизмом, позволяющим приводить в соответствие результаты двух выполненных работ. Представленный в статье подход предлагает решение, основанное на сочетании двух расширенных модулей: первый модуль полностью реализовывает требования ГОСТ и позволяет провести подбор необходимых базовых мер и провести внутреннюю оценку соответствия; второй модуль предлагает решение задачи подбора защитных мер не только в соответствии с требованиями ГОСТ, но и в том числе в зависимости от выбранного критерия оптимизации (стоимость, количество закрываемых мер), либо в зависимости от величины показателя оценки, который может дать реализация той или иной меры с помощью различных средств защиты информации. Данное решение реализовано в программном виде и находится на этапе апробации в нескольких финансовых системах.

## Литература


1. СТО БР ИББС-1.0-2014 (дата введения от 17.09.2014) [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/70567254/?ysclid=lmel9rs33r25543875 (дата обращения: 13.08.2024).

2. Киберугрозы финансовой отрасли: промежуточные итоги 2023 года [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/financial-industry-security-interim-2023/ (дата обращения: 26.08.2024).

3. Как проверить участника финансового рынка [Электронный ресурс]. URL: https://cbr.ru/finorg/ (дата обращения: 13.09.2024).

4. Козьминых, С. И. Моделирование систем и процессов защиты информации на объектах кредитно-финансовой сферы / С. И. Козьминых // Информационная безопасность финансово-кредитных организаций в условиях цифровой трансформации экономики / Под ред. С.И. Козьминых. – Москва: Общество с ограниченной ответственностью "Издательство Прометей", 2020. – С. 320-412.

5. Ситская, А. В. Автоматизация процесса проведения аудита посредством приложения "Аудит57580" / А. В. Ситская, В. В. Селифанов // Интеллектуальный потенциал Сибири: Сборник научных трудов 29-ой Региональной научной студенческой конференции, посвященной Году науки и технологий в России. В 5-ти частях, Новосибирск, 17–21 мая 2021 года / Под редакцией Д.О. Соколовой. Том Часть 5. – Новосибирск: Новосибирский государственный технический университет, 2021. – С. 607-614.

6. ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер» (Дата введения 08.08.2018) [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200146534 (дата обращения: 15.09.2024).

7. ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия» (Дата введения 28.03.2018) [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200158801 (дата обращения: 15.09.2024).

8. ГОСТ Р 57580.3-2022 «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения» (Дата введения 01.02.2023) [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200194981 (дата обращения: 25.10.2024).

9. ГОСТ Р 57580.4-2022 «Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Базовый состав организационных и технических мер» (Дата введения 01.02.2023) [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200194981 (дата обращения: 25.10.2024).

10. МП №7 «Методические рекомендации по управлению риском информационной безопасности и обеспечению операционной надежности" (Дата публикации 21.03.2024) [Электронный ресурс]. URL: https://cbr.ru/Crosscut/LawActs/File/7712 (дата обращения: 25.10.2024).

11. Банк России ответил на вопросы по исполнению требований к защите информации [Электронный ресурс]. URL: https://asros.ru/dialog/information-security/the-bank-of-russia-answered-the-questions-in-compliance-with-the-requirements-to-information-protect/ (дата обращения: 21.08.2024).

12. ЦБ оценил объем похищенных кибермошенниками денег в 4,5 млрд руб [Электронный ресурс]. URL: https://tass.ru/ekonomika/18194805 (дата обращения: 26.09.2024).

13. Лившиц, И. И. Оценка уровня обеспечения информационной безопасности в кредитной организации / И. И. Лившиц // Стандарты и качество. – 2020. – № 7. – С. 44-49.

14. Иванов, А. В. Проблемы оценки доверия к процессам аудита информационной безопасности / А. В. Иванов, И. А. Огнев // Вопросы кибербезопасности. – 2024. – № 3(61). – С. 40-50. – DOI 10.21681/2311-3456-2024-3-40-50.

15. Как повысить оценку ГОСТ 57580: быстро, эффективно, с первого раза [Электронный ресурс]. URL: https://bi.zone/expertise/events/kak-povysit-otsenku-gost-57580-bystro-effektivno-s-pervogo-raza/ (дата обращения: 12.09.2024).

16. Беляев, Е. А. Модель управления информационной безопасностью кредитных организаций / Е. А. Беляев, И. И. Лившиц // Управление финансовыми рисками. – 2023. – № 3. – С. 180-194. – DOI 10.36627/2221-7541-2023-3-3-180-194.

## References


1. STO BR IBBS-1.0-2014 (data vvedeniya ot 17.09.2014) [E`lektronny`j resurs]. URL: https://www.garant.ru/products/ipo/prime/doc/70567254/ysclid=lmel9rs33r25543875 (data obrashheniya: 13.08.2024).

2. Kiberugrozy` finansovoj otrasli: promezhutochny`e itogi 2023 goda [E`lektronny`j resurs]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/financial-industry-security-interim-2023/ (data obrashheniya: 26.08.2024).

3. Kak proverit` uchastnika finansovogo ry`nka [E`lektronny`j resurs]. URL: https://cbr.ru/finorg/ (data obrashheniya: 13.09.2024).

4. Koz`miny`x, S. I. Modelirovanie sistem i processov zashhity` informacii na ob``ektax kreditno-finansovoj sfery` / S. I. Koz`miny`x // Informacionnaya bezopasnost` finansovo-kreditny`x organizacij v usloviyax cifrovoj transformacii e`konomiki / Pod red. S.I. Koz`miny`x. – Moskva: Obshhestvo s ogranichennoj otvetstvennost`yu "Izdatel`stvo Prometej", 2020. – S. 320-412.

5. Sitskaya, A. V. Avtomatizaciya processa provedeniya audita posredstvom prilozheniya "Audit57580" / A. V. Sitskaya, V. V. Selifanov // Intellektual`ny`j potencial Sibiri: Sbornik nauchny`x trudov 29-oj Regional`noj nauchnoj studencheskoj konferencii, posvyashhennoj Godu nauki i texnologij v Rossii. V 5-ti chastyax, Novosibirsk, 17–21 maya 2021 goda / Pod redakciej D.O. Sokolovoj. Tom Chast` 5. – Novosibirsk: Novosibirskij gosudarstvenny`j texnicheskij universitet, 2021. – S. 607-614.

6. GOST R 57580.1-2017 «Bezopasnost` finansovy`x (bankovskix) operacij. Zashhita informacii finansovy`x organizacij. Bazovy`j nabor organizacionny`x i texnicheskix mer» (Data vvedeniya 08.08.2018) [E`lektronny`j resurs]. URL: https://docs.cntd.ru/document/1200146534 (data obrashheniya: 15.09.2024).

7. GOST R 57580.2-2018 «Bezopasnost` finansovy`x (bankovskix) operacij. Zashhita informacii finansovy`x organizacij. Metodika ocenki sootvetstviya» (Data vvedeniya 28.03.2018) [E`lektronny`j resurs]. URL: https://docs.cntd.ru/document/1200158801 (data obrashheniya: 15.09.2024).

8. GOST R 57580.3-2022 «Bezopasnost` finansovy`x (bankovskix) operacij. Upravlenie riskom realizacii informacionny`x ugroz i obespechenie operacionnoj nadezhnosti. Obshhie polozheniya» (Data vvedeniya 01.02.2023) [E`lektronny`j resurs]. URL: https://docs.cntd.ru/document/1200194981 (data obrashheniya: 25.10.2024).

9. GOST R 57580.4-2022 «Bezopasnost` finansovy`x (bankovskix) operacij. Obespechenie operacionnoj nadezhnosti. Bazovy`j sostav organizacionny`x i texnicheskix mer» (Data vvedeniya 01.02.2023) [E`lektronny`j resurs]. URL: https://docs.cntd.ru/document/1200194981 (data obrashheniya: 25.10.2024).

10. MP №7 «Metodicheskie rekomendacii po upravleniyu riskom informacionnoj bezopasnosti i obespecheniyu operacionnoj nadezhnosti" (Data publikacii 21.03.2024) [E`lektronny`j resurs]. URL: https://cbr.ru/Crosscut/LawActs/File/7712 (data obrashheniya: 25.10.2024).

11. Bank Rossii otvetil na voprosy` po ispolneniyu trebovanij k zashhite informacii [E`lektronny`j resurs]. URL: https://asros.ru/dialog/information-security/the-bank-of-russia-answered-the-questions-in-compliance-with-the-requirements-to-information-protect/ (data obrashheniya: 21.08.2024).

12. CzB ocenil ob``em poxishhenny`x kibermoshennikami deneg v 4,5 mlrd rub [E`lektronny`j resurs]. URL: https://tass.ru/ekonomika/18194805 (data obrashheniya: 26.09.2024).

13. Livshicz, I. I. Ocenka urovnya obespecheniya informacionnoj bezopasnosti v kreditnoj organizacii / I. I. Livshicz // Standarty` i kachestvo. – 2020. – № 7. – S. 44-49.

14. Ivanov, A. V. Problemy` ocenki doveriya k processam audita informacionnoj bezopasnosti / A. V. Ivanov, I. A. Ognev // Voprosy` kiberbezopasnosti. – 2024. – № 3(61). – S. 40-50. – DOI 10.21681/2311-3456-2024-3-40-50.

15. Kak povy`sit` ocenku GOST 57580: by`stro, e`ffektivno, s pervogo raza [E`lektronny`j resurs]. URL: https://bi.zone/expertise/events/kak-povysit-otsenku-gost-57580-bystro-effektivno-s-pervogo-raza/ (data obrashheniya: 12.09.2024).

16. Belyaev, E. A. Model` upravleniya informacionnoj bezopasnost`yu kreditny`x organizacij / E. A. Belyaev, I. I. Livshicz // Upravlenie finansovy`mi riskami. – 2023. – № 3. – S. 180-194. – DOI 10.36627/2221-7541-2023-3-3-180-194.

**ЖУКОВА Марина Николаевна,** кандидат технических наук, доцент, доцент кафедры «Безопасность информационных технологий» федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет науки и технологий имени академика Ф.М. Решетнева». 660037, Красноярский край, г. Красноярск, проспект имени газеты «Красноярский рабочий», д. 31. E-mail: zhukova@sibsau.ru

**ЯКОВЛЕВА Анастасия Олеговна,** аспирант федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет науки и технологий имени академика Ф.М. Решетнева». 660037, Красноярский край, г. Красноярск, проспект имени газеты «Красноярский рабочий», д. 31. E-mail: petrova_ao@sibsau.ru

**ZHUKOVA Marina Nikolaevna,** Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Information Technology Security of the Federal State Budgetary Educational Institution of Higher Education "Siberian State University of Science and Technology named after Academician F.M. Reshetnev". 660037, Krasnoyarsk Territory, Krasnoyarsk city, Avenue named after the newspaper "Krasnoyarsk Rabochiy", no. 31. E-mail: zhukova@sibsau.ru

**IAKOVLEVA Anastasia Olegovna,** post-graduate student of the Federal State Budgetary Educational Institution of Higher Education "Siberian State University of Science and Technology named after Academician F.M. Reshetnev". 660037, Krasnoyarsk Territory, Krasnoyarsk city, Avenue named after the newspaper "Krasnoyarsk Rabochiy", no. 31. E-mail: petrova_ao@sibsau.ru

***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(53) / 2024**
Подписано в печать 21.10.2024. Дата выхода в свет 22.10.2024.
Формат 70×108 1/16. Печать цифровая. Усл.-печ. л. 6,65. Тираж 50 экз.
Заказ 405/508.
Цена свободная.

Отпечатано в типографии Издательского центра ФГАОУ ВО «ЮУрГУ (НИУ)».
454080, г. Челябинск, пр. им. В. И. Ленина, 76, ЮУрГУ, Издательский центр.

**Bulletin of the Ural Federal District**
**Security in the Sphere of Information No. 3(53) / 2024**
Signed to print 21.10.2024. Date of publication of the 22.10.2024.
Format 70×108 1/16. Screen printing. Conventional printed sheet 6,65. Circulation – 50 issues.
Order 405/508.
Open price.

Printed in the printing house of the Publishing Center of FGAOU VO «SUSU (NIU)».
SUSU, Publishing Center, 76, Lenina Str., Chelyabinsk, 454080