

**ПРЕДСЕДАТЕЛЬ РЕДАКЦИОННОГО СОВЕТА
– ГЛАВНЫЙ РЕДАКТОР ЖУРНАЛА:**

Будко П.А. Ученый секретарь ПАО «Интелтех». Д.т.н., профессор

**ЗАМЕСТИТЕЛЬ ГЛАВНОГО РЕДАКТОРА ЖУРНАЛА
(Председатель редколлегии):**

Кулешов И.А. Заместитель генерального директора по научной работе ПАО «Интелтех». Д.т.н., доцент

ЧЛЕНЫ РЕДАКЦИОННОГО СОВЕТА:

Катанович А.А. Главный научный сотрудник НИИ ОСИСВМФ ВУНЦ ВМФ «Военно-морская академия имени Н.Г. Кузнецова». Д.т.н., профессор. Заслуженный деятель науки РФ. Заслуженный работник связи РФ. Заслуженный изобретатель РФ

Кузичкин А.В. Главный научный сотрудник Научно-исследовательского института телевидения Д.т.н., профессор. Заслуженный деятель науки РФ

Курносов В.И. Главный специалист ПАО «Интелтех». Д.т.н., профессор. Заслуженный работник связи РФ

Мирошников В.И. Генеральный конструктор ПАО «Интелтех». Д.т.н., профессор. Заслуженный деятель науки РФ

Половинкин В.Н. Научный руководитель ФГУП «Крыловский государственный научный центр». Д.т.н., профессор. Заслуженный деятель науки РФ

Присяжнюк С.П. Генеральный директор ЗАО «Институт телекоммуникаций». Д.т.н., профессор. Заслуженный деятель науки РФ

Чуднов А.М. Профессор кафедры Военной академии связи имени Маршала Советского Союза С.М. Буденного. Д.т.н., профессор

Яшин А.И. Заместитель генерального конструктора – научный руководитель работ ПАО «Интелтех». Д.т.н., профессор. Заслуженный деятель науки РФ

ЧЛЕНЫ РЕДАКЦИОННОЙ КОЛЛЕГИИ:

Винограденко А.М. Военная академия связи (г. Санкт-Петербург). Д.т.н., доцент

Габриэлян Д.Д. ФНПЦ «Ростовский-на-Дону научно-исследовательский институт радиосвязи» (г. Ростов-на-Дону). Д.т.н., профессор

Густов А.А. ПАО «Интелтех» (г. Санкт-Петербург). Д.в.н., профессор

Дорогов А.Ю. ПАО «Интелтех» (г. Санкт-Петербург). Д.т.н., доцент

Куприянов А.И. Московский авиационный институт (Национальный исследовательский университет). Д.т.н., профессор

Легков К.Е. Военно-космическая академия имени А.Ф. Можайского (г. Санкт-Петербург). К.т.н., доцент

Липатников В.А. Военная академия связи (г. Санкт-Петербург). Д.т.н., профессор

Макаренко С.И. ПАО «Интелтех» (г. Санкт-Петербург). Д.т.н., профессор

Минаков В.Ф. Санкт-Петербургский государственный экономический университет (г. Санкт-Петербург). Д.т.н., профессор

Михайлов Р.Л. Череповецкий военный ордена Жукова университет радиозлектроники (г. Череповец). Д.т.н.

Одоевский С.М. Военная академия связи (г. Санкт-Петербург). Д.т.н., профессор

Пашинцев В.П. Северо-Кавказский федеральный университет (г. Ставрополь). Д.т.н., профессор

Путилин А.Н. ПАО «Интелтех» (г. Санкт-Петербург). Д.т.н., профессор

Федоренко В.В. Северо-Кавказский федеральный университет (г. Ставрополь). Д.т.н., профессор

Финько О.А. Краснодарское высшее военное училище имени генерала армии С.М. Штеменко (г. Краснодар). Д.т.н., профессор

Цимбал В.А. Филиал Военной академии РВСН имени Петра Великого (г. Серпухов). Д.т.н., профессор

Семенов С.С. Военная академия связи (г. Санкт-Петербург). Д.т.н., профессор

Саенко И.Б. Санкт-Петербургский институт информатики и автоматизации Российской Академии Наук (г. Санкт-Петербург). Д.т.н., профессор

Стародубцев Ю.И. Военная академия связи (г. Санкт-Петербург). Д.в.н., профессор

Титков И.В. Военный учебно-научный центр Военно-Морского Флота «Военно-морская академия имени Адмирала Флота Советского Союза Н.Г. Кузнецова (г. Санкт-Петербург). Д.т.н., профессор

**EDITORIAL BOARD CHAIRMAN
– JOURNAL EDITOR-IN-CHIEF:**

Budko P.A. Academic Secretary of PJSC «Inteltech». Doctor of Technical Sciences, Professor

**JOURNAL DEPUTY EDITOR-IN-CHIEF
(Editorial Board Chairman):**

Kuleshov I.A. Deputy General Director for Scientific Work of PJSC «Inteltech». Doctor of Technical Sciences, Associate Professor

EDITORIAL COUNCIL MEMBERS:

Katanovich A.A. Chief Research Officer of the ISIS Institute of the Navy WUNCC Navy "N.G. Kuznetsov Naval Academy". Doctor of Technical Sciences, professor. Honored Inventor of the Russian Federation

Kuzichkin A.V. Chief Research Officer of the Television Research Institute. Doctor of Technical Sciences, Professor. Honored Science Worker of the Russian Federation.

Kurnosov V.I. Chief Specialist of PJSC "Inteltech". Doctor of Technical Sciences, Professor. Honored Worker of Communications of the Russian Federation.

Miroshnikov V.I. General Designer of PJSC «Inteltech». Doctor of Technical Sciences, Professor. Science Honored Worker of the Russian Federation

Polovinkin V.N. Scientific Head of FSUE Krylovsky State Scientific Center, Doctor of Technical Sciences, Professor. Honored Worker of Science of the Russian Federation

Prisyazhnik S.P. Director General of CJSC Institute telecommunications. Doctor of Technical Sciences, professor. Science Honored Worker of the Russian Federation

Chudnov A.M. Department Professor of the Communications Military Academy named after Marshal of the Soviet Union S.M. Budenniy. Doctor of Technical Sciences, Professor

Yashin A.I. Deputy General Designer – Scientific Supervisor of PJSC «Inteltech». Doctor of Technical Sciences, Professor. Science Honored Worker of the Russian Federation

EDITORIAL BOARD MEMBERS:

Vinogradenko A.M. Military Academy of Communications (St. Petersburg) Doctorate of Technical Sciences, Associate Professor

Gabrielyan D.D. FNPC "Rostov-on-Don Scientific Radio Research Institute"(Rostov-On-Don). Doctorate of Technical Sciences, Associate Professor

Gustov A.A. PJSC "Inteltech" (St. Petersburg). Doctor of Military Sciences, Professor

Dorogov A.Y. PJSC "Inteltech" (St. Petersburg). Doctor of Technical Sciences, Associate Professor

Kupriyanov A.I. Moscow Aviation Institut (National Research Universit) Doctor of Technical Sciences, Professor

Legkov C.E. Military Space Academy of A.F. Mozhaiskiy (St. Petersburg). Doctorate of Technical Sciences, Associate Professor

Lipatnikov V.A. Military Academy of Communications (St. Petersburg). Doctor of Technical Sciences, Professor

Makarenko S.I. PJSC "Inteltech" (St. Petersburg). Doctor of Technical Sciences, Professor

Minakov V.F. St. Petersburg State Economic University (St. Petersburg). Doctor of Technical Sciences, Professor

Mikhailov R.L. Cherepovets Military Order of Zhukov University of Asche Radioelectronics (Cherepovets). Doctorate of Technical Sciences. Associate Professor.

Odoevsky S.M. Military Academy of Communications (St. Petersburg). Doctor of Technical Sciences, Professor

Pashintsev V.P. North Caucasus Federal University (Stavropol). Doctor of Technical Sciences, Professor

Putilin A.N. PJSC "Inteltech" (St. Petersburg). Doctor of Technical Sciences, Professor

Fedorenko V.V. North Caucasus Federal University. (Stavropol). Doctor of Technical Sciences, professor

Finko O.A. Krasnodar Higher Military School named after General of the Army S.M. Stemenko (Krasnodar). Doctor of Technical Sciences, Professor

Tsymbal V.A. Branch of the Great Petr RVSNI Military Academy (Serpukhov). Doctor of Technical Sciences, Professor

Semenov S.S. Military Academy of Communications (St. Petersburg). Doctor of Technical Sciences, Professor

Saenko I.B. Saint Petersburg Institute of Informatics and Automation of the Sciences Russian Academy (St. Petersburg). Doctor of Technical Sciences, Professor

Starodubtsev Y.I. Military Academy of Communications (St. Petersburg). Doctor of Military Sciences, Professor

Titkov I.V. Military Educational and Scientific Center of the Navy "Naval Academy named after Admiral of the Fleet of the Soviet Union N.G. Kuznetsov (St. Petersburg). Doctor of Technical Sciences, Professor

РЕДАКЦИЯ:

Верстка принт-макета: **Тюкинеева Л.В.**
Дизайн обложки: **Шаутин Д.В.**
Поддержка сетевой версии журнала: **Тюкинеева Л.В.**
Секретарь редакции: **Тюкинеева Л.В.**

**АДРЕС
РЕДАКЦИИ:**

197342. Россия. г. Санкт-Петербург, ул. Кантемировская, дом 8,
Телефон: +7(812) 542-90-54; +7(812) 448-95-97; +7(812) 448-96-84
Факс: +7(812) 542-18-49. E-mail: mce-journal@inteltech.ru.
Официальный сайт: www.inteltech.ru; www.mce-journal.ru



Научно-технический журнал «Техника средств связи» – это рецензируемое научное издание, в котором публикуются результаты научных исследований специалистов в области современных инфокоммуникационных технологий и автоматизированных систем управления, средств связи и информационной безопасности. Журнал является правопреемником издававшихся с 1959 года Министерством промышленности средств связи СССР всеобщих журналов «Вопросы радиоэлектроники. Серия: Техника проводной связи» и «Вопросы специальной радиоэлектроники. Серия: Техника проводной связи». С 1975 года журнал издается под названием «Техника средств связи». Учредитель и издатель журнала: Публичное акционерное общество «Информационные телекоммуникационные технологии» (ПАО «Интелтех»). Адрес учредителя и издателя журнала: 197342, Россия, г. Санкт-Петербург, ул. Кантемировская, д.8.

Адрес типографии: 623102, Свердловская область, г. Первоуральск. пр. Ильича д.26А, АО «Первоуральская типография».

Главный редактор журнала-Председатель редакционного совета - П.А. Будко, Ученый секретарь ПАО «Интелтех», Д.т.н., профессор.

Решением ВАК № 222-р от 10.06.2024 научно-технический журнал «Means of communication equipment» («Техника средств связи») включен в перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук и рекомендован ВАК для публикаций основных результатов по научным специальностям: 2.2.13. Радиотехника, в том числе системы и устройства телевидения; 2.2.14. Антенны, СВЧ устройства и их технологии; 2.2.15. Системы, сети и устройства телекоммуникаций; 2.3.1. Системный анализ, управление и обработка информации, статистика; 2.3.5. Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей; 2.3.6. Методы и системы защиты информации, информационная безопасность (по отраслям науки - технические науки).

Выходит 4 раза в год.

Публикация в журнале является научным печатным трудом.

Основное содержание издания представляет собой научные статьи и научные обзоры.

Возрастное ограничение 12 +

Журнал зарегистрирован как сетевое и печатное издания в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Свидетельства о регистрации средств массовой информации: ПИ № ФС 77 – 80135 и ЭЛ № ФС 77 – 80136 от 31.12.2020 г.

ISSN (print): 2782-2141; ISSN (online): 2782-2133; РИНЦ (eLIBRARY ID: 77074)

Распространяется по подписке. Подписной индекс журнала-79656. Ссылки для оформления интернет-подписки на журнал:

<https://www.akc.ru/itm/means-of-communication-equipment/>; <https://www.pressa-rf.ru/cat/1/edition/e79656/>

Свободная цена

Тираж: 40 экз.

Подписано в печать 19.06.2026. Дата выхода в свет 22.06.2026.

СОДЕРЖАНИЕ

СИСТЕМЫ СВЯЗИ И ТЕЛЕКОММУНИКАЦИИ

- Негурица А. О. 2
Модель формирования и приема сигналов для анализа и оптимизации помехоустойчивости канала передачи данных в условиях преднамеренных и случайных помех
Сулима А. А., Калямин И. В. 11
Развитие аппаратуры и систем связи на основе технологии когнитивного радио

ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Фаткеева Р. Р., Билятдинов К. З., Фортинский А. Г. 21
Метод оценки защищенности информации и информационной безопасности объекта критической информационной инфраструктуры
Фаткеева Р. Р., Билятдинов К. З., Фортинский А. Г. 31
Метод управления информационной безопасностью и восстановления информационных систем на основе реконфигурации объекта критической инфраструктуры
Смирнов С. В., Усовик С. В., Герасимова Е. Г., Сергеев В. Ю., Шкаренкова А. М. 39
Изолированная архитектура для воспроизводимых исследований противодействия удаленному управлению
Митрофанов М. В., Крамской Н. Н., Куракин А. С., Густов А. А. 54
Применение архитектуры zero trust для обеспечения информационной безопасности больших языковых моделей в корпоративной инфраструктуре

ИНТЕЛЛЕКТУАЛЬНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

- Чижов А. С. 65
Анализ применения нейросетевых методов для улучшения точности локального позиционирования на основе радиочастотных отпечатков в стандартах IEEE 802.11
Аменицкий А. В., Воробьев Е. Г. 75
Управление рисками искусственного интеллекта: концептуальная модель проактивной безопасности в условиях киберпреступности с использованием искусственного интеллекта

ЭЛЕКТРОННЫЕ И РАДИОТЕХНИЧЕСКИЕ СИСТЕМЫ

- Баранов А. А., Егоров В. В. 82
Оптимизация выходного сигнала ключевого генератора СДВ диапазона при относительной фазовой телеграфии

РОБОТОТЕХНИЧЕСКИЕ СИСТЕМЫ

- Будко Д. Д. 90
Оценка помехоустойчивости сигнально-кодовых конструкций команд управления беспилотными транспортными средствами на основе технологий расширения спектра

CONTENTS

COMMUNICATION AND TELECOMMUNICATION SYSTEMS

- Neguritsa A. O. 2
Model for generating and receiving signals for analyzing and optimizing the noise immunity of a data transmission channel in the presence of intentional and random interference
Sulima A. A., Kalyamin I. V. 11
Development of communication equipment and systems based on cognitive radio technology

INFORMATION SECURITY ISSUES

- Fatkееva R. R., Bilyatdinov K. Z., Fortinsky A. G. 21
Method for assessing the information security of a critical information infrastructure facility
Fatkееva R. R., Bilyatdinov K. Z., Fortinsky A. G. 31
Method for managing information security and restoring information systems based on reconfiguration of a critical infrastructure facility
Smirnov S. V., Usovik S. V., Gerasimova E. G., Sergeenkov V. Yu., Shkarenkova A. M. 39
An isolated architecture for reproducible research on countering remote control
Mitrofanov M. V., Kurakin A. S., Kramskoy N. N., Gustov A. A. 54
Application of zero trust architecture to ensure information security of large language models in corporate infrastructure

INTELLIGENT INFORMATION SYSTEMS

- Chizhov A. S. 65
Analysis of the use of neural network methods to improve the accuracy of local positioning based on radio frequency fingerprints in IEEE 802.11 standards
Amenitsky A. V., Vorobyov E. G. 75
Artificial intelligence risk management: conceptual model of proactive security in conditions of ai-enabled cybercrime

ELECTRONIC AND RADIO ENGINEERING SYSTEMS

- Baranov A. A., Egorov V. V. 82
Optimization of the output signal of the key range shift generator in relative phase telegraphy

ROBOTIC SYSTEMS

- Budko D. D. 90
Evaluation of the noise immunity of signal-code structures of unmanned vehicle control commands based on spectrum expansion technologies

Рубрики журнала: Анализ новых технологий и перспектив развития техники средств связи • Системы управления • Передача, прием и обработка сигналов • Системы связи и телекоммуникации • Перспективные исследования • Вычислительные системы • Информационные процессы и технологии. Сбор, хранение и обработка информации • Моделирование сложных организационно-технических систем • Вопросы обеспечения информационной безопасности • Интеллектуальные информационные системы • Робототехнические системы • Электронные и радиотехнические системы • Объекты интеллектуальной собственности и инновационные технологии в области разработки средств телекоммуникаций

СИСТЕМЫ СВЯЗИ И ТЕЛЕКОММУНИКАЦИИ

УДК 621.391.8

DOI: 10.24412/2782-2141-2026-2-2-10

**Модель формирования и приема сигналов для анализа
и оптимизации помехоустойчивости канала передачи данных
в условиях преднамеренных и случайных помех**

Негурица А. О.

Аннотация. Постановка задачи. Требуется построить и исследовать модель приема двоичных сигналов на физическом уровне канала связи в условиях случайного шума и преднамеренного воздействия, обеспечить получение аналитических зависимостей вероятности ошибки для различных режимов помехи и сформировать показатель качества, отражающий наихудший сценарий при ограниченных возможностях нарушителя. **Целью работы** является получение гарантированной оценки вероятности ошибки на бит и анализ влияния помеховой обстановки и выбранного решающего правила приема на устойчивость канала передачи данных. **Используемые методы.** Применены статистическое моделирование на уровне решающей статистики после корреляционной (согласованной) обработки, вероятностный анализ и вывод аналитических выражений для вероятности ошибки, а также подход гарантированной оценки качества связи в постановке «наихудший нарушитель» при ресурсных ограничениях. **Новизна** состоит в совместном рассмотрении некогерентной преднамеренной помехи и рандомизированного порогового решающего правила приема, а также во введении гарантированной (наихудшей) вероятности ошибки как метрики для сопоставления вариантов приема при ограниченном ресурсе воздействия. **Результат:** получена дискретная статистическая модель канала и аналитические зависимости вероятности ошибки на бит для когерентного и некогерентного режимов помехи; сформирована гарантированная оценка качества приема, позволяющая корректно сравнивать варианты приема и исследовать влияние параметров помеховой обстановки и алгоритма принятия решения. **Практическая значимость:** предложенная модель может использоваться для аналитической оценки помехоустойчивости физического уровня, обоснования требований к устойчивости канала связи и выбора/настройки приемных решений при работе в условиях совместного действия случайных и преднамеренных помех.

Ключевые слова: канал передачи данных, помехоустойчивость, преднамеренная помеха, АБГШ, когерентный/некогерентный прием, рандомизированное решающее правило приема, вероятность ошибки на бит, гарантированная вероятность ошибки, ресурсное ограничение.

Актуальность

Настоящая работа посвящена исследованию методов анализа и выбора параметров обработки сигналов на физическом уровне канала передачи данных, функционирующего в условиях преднамеренных помех и аддитивного белого гауссовского шума, при этом преднамеренная помеха моделируется как воздействие, направленное на ухудшение показателей приёма.

Вопросы оценки гарантированных показателей качества передачи информации в условиях преднамеренных помех достаточно подробно отражены в литературе [1-16]. При этом значительная часть работ ориентирована на анализ когерентного воздействия, предполагающего согласование помехи с полезным сигналом или решающей статистикой приёмника. Вместе с тем для практических сценариев существенный интерес представляет рассмотрение некогерентной преднамеренной помехи, характеризуемой неопределённостью фазовых (и/или амплитудных) параметров относительно полезного сигнала, а также получение аналитических зависимостей вероятности ошибки на бит на выходе демодулятора в условиях такого воздействия.

В отличие от типовой когерентной постановки, в работе рассмотрен случай некогерентной преднамеренной помехи, когда фаза помехового колебания на интервале символа является неизвестной (случайной) величиной. Для данного режима получены

аналитические выражения для вероятности ошибки на бит путём усреднения по фазе, что обеспечивает сопоставимость с когерентным случаем в рамках единой метрики качества.

Дальнейшее изложение сосредоточено на построении модели канала передачи данных на физическом уровне, позволяющей связать вероятность ошибки на бит на выходе демодулятора с параметрами помеховой обстановки и параметрами алгоритма принятия решений. Решающая статистика формируется с использованием корреляционной обработки (согласованного приёма) на интервале передачи: непрерывный принимаемый сигнал проецируется на известные приёмнику опорные функции, в результате чего получается дискретный набор корреляционных коэффициентов. Такое представление переводит модель в дискретную форму и даёт возможность явно учитывать вклад аддитивного белого гауссовского шума и преднамеренной помехи в решающую статистику, обеспечивая корректное получение зависимостей ошибки от рассматриваемых параметров.

Преднамеренная помеха задаётся через ресурсное ограничение по средней мощности: вводятся нормированная мощность воздействия d и параметр ограничения δ , причём выполняется условие $E[d] \leq \delta$. Такая постановка обеспечивает возможность анализа, как при фиксированном уровне воздействия, так и при ограниченном среднем ресурсе помехи, а также позволяет сопоставлять различные режимы воздействия, включая когерентный и некогерентный.

Особенностью используемого алгоритма приёма является Δ -слой – рандомизированное решающее правило приема, введенный и описанный в [5, 6]. На основе указанного правила выводятся зависимости вероятности ошибки на бит $P_e(d, \phi, \sigma, \Delta)$ и исследуется влияние параметров $d, \delta, \sigma, \Delta$ на помехоустойчивость физического уровня при некогерентном режиме преднамеренной помехи (с рассмотрением когерентного режима в качестве предельного случая).

Постановка задачи

Целью исследования является получение гарантированной (наихудшей) оценки вероятности ошибки на бит и её интерпретация с точки зрения влияния параметров помеховой обстановки и алгоритма принятия решений на устойчивость физического уровня при наличии преднамеренного нарушителя. Для достижения цели решаются следующие задачи:

- формализовать дискретную модель решающей статистики на основе корреляционной обработки и рандомизированного порогового правила с параметром Δ ;
- задать класс допустимых стратегий нарушителя $V(\delta)$ при ограничении по средней мощности $E[d] \leq \delta$ и описать когерентный и некогерентный режимы воздействия;
- получить выражения для $P_e(d, \phi, \sigma, \Delta)$ и рассмотреть частные случаи;
- определить гарантированную (наихудшую) вероятность ошибки на бит как максимум по классу допустимых воздействий и исследовать её зависимость от параметров δ, σ и Δ , а также выполнить численный анализ.

Таким образом, решаемая задача построения модели включает:

- формирование общей математической конструкции U_f , описывающей класс рассматриваемых вариантов приёмной на физическом уровне и правило принятия решений с параметром Δ ;
- формализованное описание класса $V(\delta)$ допустимых преднамеренных воздействий, ограниченных по средней мощности: $E[d] \leq \delta$;
- получение гарантированной (наихудшей) вероятности ошибки на бит P_e^* как наихудшего значения по классу допустимых воздействий и анализ ее свойств [1, 2]:

$$P_e^*(U_f, \delta, \sigma) = \sup_{V \in V(\delta)} P_e(U_f, V, \sigma) .$$

Модель канала передачи данных

Рассматриваемая система передачи данных включает передающую часть, канал прямой связи и приёмную часть, а также канал обратной связи для передачи служебной информации о результате приёма.

Входной последовательности двоичных символов $\{a_i\}$, $a_i \in \{0,1\}$, сопоставлен непрерывный передаваемый сигнал $s(t)$, формируемый модулятором. Далее сигнал подвергается частотному преобразованию в блоке псевдослучайной перестройки рабочей частоты (ППРЧ), после чего распространяется по каналу прямой связи в условиях аддитивного воздействия преднамеренной помехи $v(t)$ и аддитивного белого гауссовского шума $\xi(t)$:

$$u(t) = s(t) + v(t) + \xi(t),$$

где $u(t)$ – сигнал на входе демодулятора.

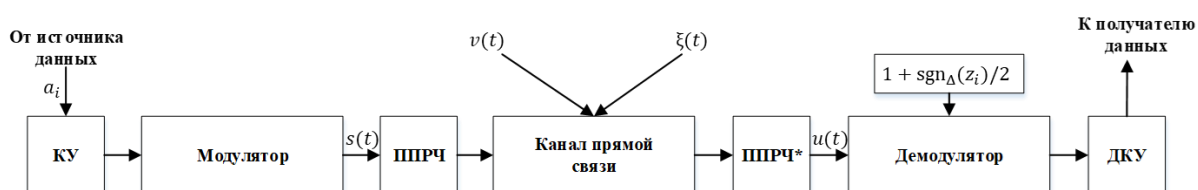


Рис. 1. Канал передачи данных

Преднамеренная помеха $v(t)$ рассматривается как аддитивное воздействие нарушителя на вход демодулятора. Интенсивность воздействия далее параметризуется нормированной текущей мощностью d , определяемой на интервале символа и используемой при построении зависимостей вероятности ошибки. Аддитивный белый гауссовский шум (АБГШ) моделируется как статистически независимый от полезного сигнала и преднамеренной помехи.

На приемной стороне выполняется согласованное обратное частотное преобразование (ППРЧ*), затем принятие решения выполняется по рандомизированному решающему правилу Δ -слоя неразличимости

$$\text{sgn}_{\Delta}(u) = \begin{cases} -1, u < -\Delta \\ 0, |u| \leq \Delta \\ 1, u > \Delta \end{cases}, \quad (1)$$

где при $|u| \leq \Delta$ решение одно из значений $+1$ или -1 выбирается случайно с вероятностью $0,5$ [5, 6, 8].

Для обеспечения корректного сопоставления «с Δ -слоем / без Δ -слоя» базовый случай далее отождествляется с $\Delta = 0$ (Δ -слой отсутствует, рассматривается приемник Котельникова), а при $\Delta > 0$ соответствует приему с Δ -слоем.

Для дальнейшего анализа вводятся входные и выходные процессы каждого функционального блока, что обеспечивает переход к дискретной статистической модели наблюдений и последующему выводу выражений для вероятности ошибки на бит P_e .

Далее рассмотрена дискретная модель на уровне решающей статистики, формируемой после согласованной (корреляционной) обработки на интервале символа. Непрерывное наблюдение на каждом интервале проецируется на опорные функции, в результате чего формируется скалярная статистика z_j , по которой принимаем решение на j -м бите согласно (1). Вероятность ошибки P_e , выводимая далее, относится к выходу демодулятора (после коррелятора и правила принятия решения) и определяется распределением z_j при наличии помехи и АБГШ.

После согласованной корреляционной обработки принимаемого колебания формируется решающая статистика u_j для j -го бита как скалярный функционал наблюдения на интервале символа:

$$u_j = \int_0^{T_s} u(t) \psi_j(t) dt, \quad j = 1, 2, \dots,$$

где $\psi_j(t)$ – опорная функция, $\int_0^{T_s} \psi_j^2(t) dt = 1$.

При принятой нормировке полезная составляющая на выходе коррелятора имеет вид $s_j \in \{+1, -1\}$, а шумовая компонента после корреляционной обработки является гауссовской: $\xi_j \sim N(0, \sigma^2)$.

Влияние преднамеренного воздействия определяется проекцией помехи на решающее направление приемника:

$$v_j = \langle v, \psi_j \rangle,$$

и, используя параметризацию через нормированную мощность $d \geq 0$ и фазовый параметр φ , записывается в виде

$$v = \sqrt{d} \cos \varphi,$$

где d – нормированная текущая мощность помехи.

Когерентное воздействие помехи соответствует фиксированному фазовому соотношению $\varphi = \text{const}$, т. е. детерминированной проекции v . В постановке наихудшего случая выбирается фазовая ориентация, минимизирующая разделимость гипотез, это соответствует $\varphi = \pi$, $\cos \varphi = -1$, следовательно

$$u_j = s_j - \sqrt{d} + \xi_j.$$

Некогерентное воздействие помехи описывает отсутствие фазового согласования, при котором $\varphi \sim U(0, \pi)$:

$$u_j = s_j + \sqrt{d} \cos \varphi + \xi_j. \quad (2)$$

В качестве оценки показателя эффективности устойчивости к помехам проведены расчеты вероятности ошибки на бит P_e с введением Δ -слоя неразличимости. В общем случае фазовое соотношение моделируется случайной величиной, тогда P_e определяется усреднением условной вероятности по φ :

$$P_e^{\text{общ}}(d, \sigma, \Delta) = E_{\varphi} \{P_e(d, \sigma, \Delta, \varphi)\} = \frac{1}{\pi} \int_0^{\pi} P_e(d, \sigma, \Delta, \varphi) d\varphi.$$

Исходя из (1) P_e выражено через условную вероятность ошибки при передаче символа:

$$P_e(d, \varphi, \sigma, \Delta) = \Pr\{u_j < -\Delta \mid s_j = +1\} + \frac{1}{2} \Pr\{-\Delta \leq u_j \leq \Delta \mid s_j = +1\}.$$

Из (2) при $s_j = +1$ получаем

$$u_j = 1 + \sqrt{d} \cos \varphi + \xi_j.$$

Пусть $1 + \sqrt{d} \cos \varphi = \mu$, тогда введена нормальная величина:

$$Z = \frac{u_j - \mu}{\sigma} \sim N(0, 1), \quad \Phi(x) = \Pr\{Z \leq x\}.$$

Для $\Pr\{u_j < -\Delta \mid s_j = +1\}$

$$\Pr\{u_j < -\Delta\} = \Pr\left\{\frac{u_j - \mu}{\sigma} < \frac{-\Delta - \mu}{\sigma}\right\} = \Phi\left(\frac{-\Delta - \mu}{\sigma}\right);$$

подставляем $\mu = 1 + \sqrt{d} \cos \varphi$, получаем

$$\Pr\{u_j < -\Delta \mid s_j = +1\} = \Phi\left(\frac{-\Delta - 1 - \sqrt{d} \cos \varphi}{\sigma}\right). \quad (3)$$

Для $\Pr\{-\Delta < u_j < \Delta \mid s_j = +1\}$ имеем

$$\Pr\{-\Delta < u_j < \Delta \mid s_j = +1\} = \Pr\{u_j < \Delta\} - \Pr\{u_j < -\Delta\},$$

что эквивалентно

$$\begin{aligned} \Pr\{-\Delta < u_j < \Delta \mid s_j = +1\} &= \Phi\left(\frac{\Delta - \mu}{\sigma}\right) - \Phi\left(\frac{-\Delta - \mu}{\sigma}\right) = \\ &= \Phi\left(\frac{\Delta - 1 - \sqrt{d} \cos \varphi}{\sigma}\right) - \Phi\left(\frac{-\Delta - 1 - \sqrt{d} \cos \varphi}{\sigma}\right). \end{aligned} \quad (4)$$

Из (3) и (4) получаем общую формулу

$$P_e(d, \varphi, \sigma, \Delta) = \Phi\left(\frac{-\Delta - 1 - \sqrt{d} \cos \varphi}{\sigma}\right) + \frac{1}{2} \left[\Phi\left(\frac{\Delta - 1 - \sqrt{d} \cos \varphi}{\sigma}\right) - \Phi\left(\frac{-\Delta - 1 - \sqrt{d} \cos \varphi}{\sigma}\right) \right].$$

Частный случай когерентного воздействия помехи, при условии, что $\varphi = \pi \Rightarrow \cos \varphi = -1$, представлен в следующем виде:

$$P_e^{(\text{ког})}(d, \sigma, \Delta) = \Phi\left(\frac{-\Delta - 1 + \sqrt{d}}{\sigma}\right) + \frac{1}{2} \left[\Phi\left(\frac{\Delta - 1 + \sqrt{d}}{\sigma}\right) - \Phi\left(\frac{-\Delta - 1 + \sqrt{d}}{\sigma}\right) \right].$$

Преднамеренная помеха формируется при ресурсном ограничении по средней мощности: для нормированной текущей мощности воздействия d выполняется условие $E[d] \leq \delta$. В этих условиях качество связи оценивается наихудшей вероятностью ошибки на бит

$$P^\wedge(\delta \mid \Delta) = \sup_{F_d: E[d] \leq \delta} E_d[P(d, \sigma, \Delta)],$$

где F_d – стратегия выбора текущей мощности d по интервалам символов.

Таким образом получена аналитическая зависимость $P(d, \sigma, \Delta)$ для когерентного и некогерентного воздействия помехи и задана гарантированная вероятность ошибки $P^\wedge(\delta \mid \Delta)$ для сопоставления приемника Котельникова и приемника с Δ -слоем.

Результаты моделирования

Численные зависимости получены путем расчета по аналитическим выражениям на равномерной сетке по мощности воздействия $d \in [0, D_{\max}]$ с шагом $\Delta d = D_{\max} / N$ (в работе использовано $D_{\max} = 2,6$; $N = 600$). Вероятность ошибки $P(d \mid \Delta)$ вычислялась по полученной формуле через нормальную функцию распределения для набора $\Delta \in \{0, 0.1, 0.1716, 0.3\}$ и заданных значений σ , $P^\wedge(\delta \mid \Delta)$ строилась как верхняя выпуклая оболочка [2], что соответствует оценке при ограничении по среднему ресурсу.

На рис. 2 – 5 приведены зависимости текущей вероятности ошибки на бит $P(d \mid \Delta)$ (сплошные линии) и гарантированной вероятности ошибки на бит $P^\wedge(\delta \mid \Delta)$ (пунктирные линии) от параметров d и δ для определенных значений Δ . Для сопоставления представлены результаты как для когерентного воздействия помехи (фиксированная фаза, наихудший случай), так и для некогерентного воздействия (отсутствие фазового согласования, усреднение по фазе).

Из полученных зависимостей следуют следующие закономерности:

- при увеличении текущей мощности воздействия d вероятность ошибки $P(d \mid \Delta)$ возрастает, что соответствует ухудшению разделимости гипотез на выходе коррелятора при росте проекции помехи на решающее направление;

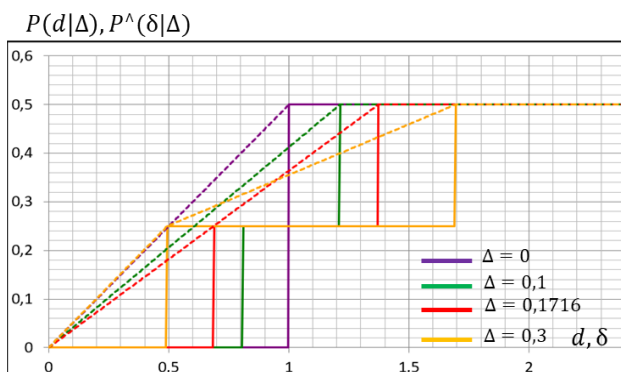


Рис. 2. Зависимость величин $P(d|\Delta)$, $P^\wedge(\delta|\Delta)$ от значений d , δ текущей и средней мощности при $\sigma = 0$

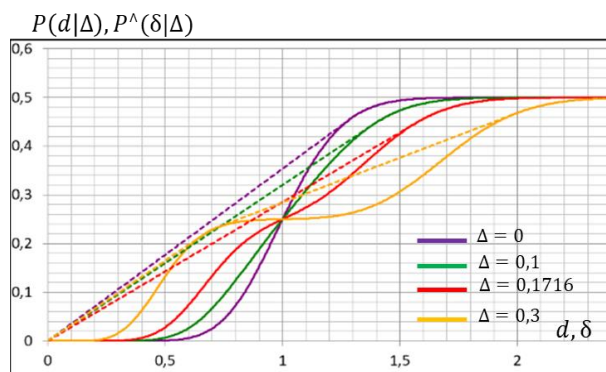


Рис. 3. Зависимость величин $P(d|\Delta)$, $P^\wedge(\delta|\Delta)$ от значений d , δ текущей и средней мощности при $\sigma = 0,1$

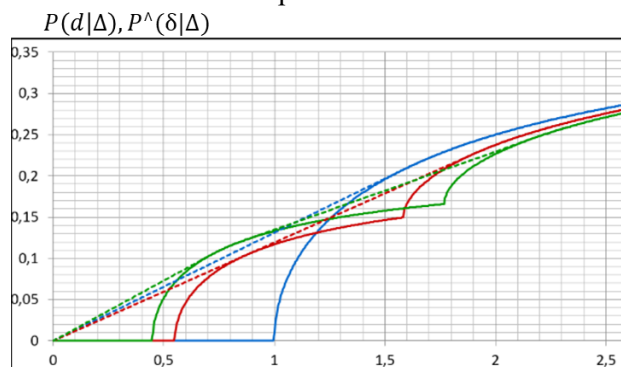


Рис. 4. Зависимость величин $P(d|\Delta)$, $P^\wedge(\delta|\Delta)$ от значений d , δ текущей и средней мощности при $\sigma = 0$

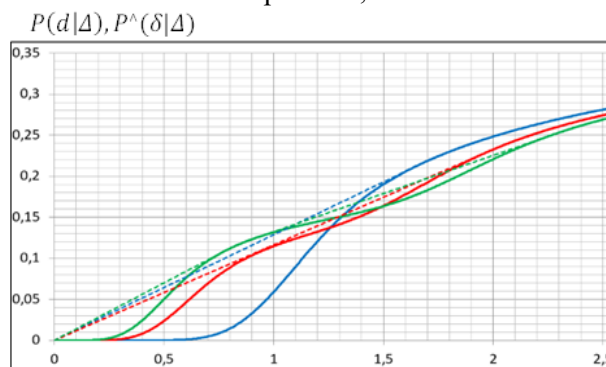


Рис.5 – Зависимость величин $P(d|\Delta)$, $P^\wedge(\delta|\Delta)$ от значений d , δ текущей и средней мощности при $\sigma = 0,1$

- гарантированная вероятность ошибки $P^\wedge(\delta|\Delta)$, определенная как наихудшее значение по классу стратегий нарушителя $E[d] \leq \delta$, является интегральной характеристикой устойчивости и обеспечивает корректное сравнение режимов «фиксированная мощность/ограниченный средний ресурс»;
- введение рандомизированного решающего правила приема приводит к изменению зависимостей $P(d|\Delta)$ и $P^\wedge(\delta|\Delta)$ по сравнению с приемником Котельникова, что позволяет параметрически настраивать область рандомизации для достижения требуемого компромисса между устойчивостью к воздействию и чувствительностью к шуму;
- для некогерентного режима зависимости $P(d|\Delta)$ и $P^\wedge(\delta|\Delta)$ отличаются по сравнению с когерентным случаем: вследствие усреднения по фазе изменяется эффективность проекции помехи на решающее направление коррелятора, поэтому экстремальные значения вероятности ошибки достигаются при иных значениях d и δ . Это подчеркивает, что предположение о когерентной помехе соответствует наиболее неблагоприятному сценарию и может рассматриваться как верхняя оценка деградации при практической фазовой неопределенности;
- увеличение уровня шума σ приводит к росту $P(d|\Delta)$ и $P^\wedge(\delta|\Delta)$ во всем диапазоне d , δ , при этом влияние Δ становится более заметным в переходной области, где вероятность ошибки изменяется от малых значений к насыщению;
- сопоставление $P(d|\Delta)$ и $P^\wedge(\delta|\Delta)$ показывает, что ограничение по среднему ресурсу нарушителя приводит к более консервативной оценке качества связи по сравнению с фиксированным d , что оправдывает использование гарантированной метрики при анализе противодействия преднамеренным помехам.

Выводы

Разработанная модель канала связи в условиях аддитивной преднамеренной помехи и АБГШ предназначена для аналитической оценки вероятности ошибки на бит на выходе демодулятора и исследования влияния параметров помеховой обстановки и приемного алгоритма. Модель позволяет вычислять зависимость $P(d, \sigma, \Delta)$ и тем самым прогнозировать качество приема при заданном текущем уровне воздействия d и уровне шума σ ; выполнять сопоставление базового приемника ($\Delta = 0$) и приема с Δ -слоем ($\Delta > 0$) по вероятности ошибки; выбирать и параметрически настраивать Δ -слой для обеспечения требуемого уровня помехоустойчивости при заданных условиях; оценивать устойчивость системы в постановке «наихудшего нарушителя» при ограничении по среднему ресурсу мощности $E[d] \leq \delta$ через гарантированную метрику $P^*(\delta|\Delta)$. Тем самым модель может использоваться как основа для дальнейшего численного анализа и выработки практических рекомендаций по настройке приемника и оценке допустимых уровней преднамеренного воздействия.

Литература

1. Чуднов А. М. Теоретико-игровые задачи синтеза алгоритмов формирования и приема сигналов // Проблемы передачи информации. 1991. Т. 27, № 3. С. 57–65.
2. Чуднов А. М. Математические основы моделирования, анализа и синтеза систем. Санкт-Петербург: Военная академия связи, 2021. 193 с.
3. Chudnov A. M., Kichko Ya. V., Sapunova L. P. Optimization of the guaranteed rate of information transmission by pseudo-random signals with a randomized base under conditions of deliberate interference // Radio Engineering and Electronics. 2023. Vol. 68, No. 3. P. 263–270.
4. Глушанков Е. И., Кирик Д. И., Кондрашов З. К., Рылов Е. А., Морозов А. А. Анализ помехоустойчивости локальных систем морской навигации в условиях воздействия оптимизированных помех // Морской вестник. 2025. № 1 (93). С. 89–91.
5. Chudnov A. M., Sazonov V. V., Bikbulatov V. R. Optimization of the decisive rule for a receiver with a Δ -layer of indistinguishability of binary signals in a channel with intentional interference // Problems of Information Transmission. 2025. Vol. 61, No. 1. P. 41–55.
6. Чуднов А. М., Сазонов В. В., Бикбулатов В. Р. Оптимизация области неразличимости приемником двоичных сигналов, передаваемых по каналу с преднамеренной помехой // Проблемы передачи информации. 2025. Т. 61, № 1. С. 47–59.
7. Савищенко Н. В. Помехоустойчивость когерентного приема многопозиционных сигналов КАМ и ФМ при неидеальной синхронизации // Информационно-управляющие системы. 2010. № 1 (44). С. 53–63.
8. Негурица А. О. Оценка эффективности использования Δ -слоя неразличимости двоичных сигналов, принимаемых в условиях случайных и преднамеренных помех // Телекоммуникации и связь. 2025. № 4 (07). С. 22–27.
9. Cahn C. Worst interference for coherent binary channel // IEEE Transactions on Information Theory. 1971. Vol. 17, No. 2. P. 209–210. doi:10.1109/TIT.1971.1054597.
10. Вейцель В. А., Жодзишский М. И., Жодзишский Ю. И. Гарантированная помехоустойчивость приема сигналов // Радиотехника и электроника. 1987. Т. 32, № 2. С. 316–321.
11. Bashar T., Wu Y.-W. A complete characterization of minimax and maximin encoder-decoder policies for communication channels with incomplete statistical description // IEEE Transactions on Information Theory. 1985. Vol. 31, No. 4. P. 482–489. doi:10.1109/TIT.1985.1057076.
12. Путилин А. Н., Чуднов А. М. Оптимизация приемника фазоманипулированных псевдослучайных сигналов при наихудшей помехе с ограниченной средней мощностью // Радиотехника и электроника. 1990. Т. 35, № 8. С. 1646–1650.
13. Kullstam P. Spread spectrum performance analysis in arbitrary interference // IEEE Transactions on Communications. 1977. Vol. 25, No. 8. P. 848–853. doi:10.1109/TCOM.1977.1093906.
14. Zhou S., Giannakis G. B., Swami A. Digital multi-carrier spread spectrum versus direct sequence spread spectrum for resistance to jamming and multipath // IEEE Transactions on Communications. 2002. Vol. 50, No. 4. P. 643–655. doi:10.1109/26.996079.

15. Poisel R. A. Modern communications jamming: principles and techniques. Boston: Artech House, 2011.
16. Li S. Concise formulas for the area and volume of a hyperspherical cap // Asian Journal of Mathematics and Statistics. 2011. Vol. 4, No. 1. P. 66–70. doi:10.3923/ajms.2011.66.70.

References

1. Chudnov A. M. *Teoretiko-igrovyye zadachi sinteza algoritmov formirovaniya i priema signalov* [Game-theoretic problems of synthesis of algorithms for generating and receiving signals]. *Problemy peredachi informacii*, 1991, v. 27, no. 3, pp. 57–65 (in Russian).
2. Chudnov A. M. *Matematicheskie osnovy modelirovaniya, analiza i sinteza sistem* [Mathematical foundations of modeling, analysis and synthesis of systems]. Sankt-Peterburg. Military Academy of Communications publ., 2021. 193 p. (in Russian).
3. Chudnov A. M., Kichko Ya. V., Sapunova L. P. *Optimization of the guaranteed rate of information transmission by pseudo-random signals with a randomized base under conditions of deliberate interference* [Optimization of the guaranteed rate of information transmission by pseudo-random signals with a randomized base under conditions of deliberate interference]. *Radio Engineering and Electronics*, 2023, v. 68, no. 3, pp. 263–270.
4. Glushankov E. I., Kirik D. I., Kondrashov Z. K., Rylov E. A., Morozov A. A. *Analiz pomexoustojchivosti lokal'nykh sistem morskoy navigacii v usloviyax vozdejstviya optimizirovannykh pomex* [Analysis of noise immunity of local marine navigation systems under conditions of optimized interference]. *Morskoy vestnik*, 2025, no. 1 (93), pp. 89–91 (in Russian).
5. Chudnov A. M., Sazonov V. V., Bikbulatov V. R. *Optimization of the decisive rule for a receiver with a Δ -layer of indistinguishability of binary signals in a channel with intentional interference* [Optimization of the decisive rule for a receiver with a Δ -layer of indistinguishability of binary signals in a channel with intentional interference]. *Problems of Information Transmission*, 2025, v. 61, no. 1, pp. 41–55.
6. Chudnov A. M., Sazonov V. V., Bikbulatov V. R. *Optimizatsiya oblasti nerazlichimosti priemnikom dvoichnykh signalov, peredavaemykh po kanalu s prednamerennoy pomexoj* [Optimization of the area of indistinguishability by the receiver of binary signals transmitted over a channel with deliberate interference]. *Problemy peredachi informacii*, 2025, v. 61, no. 1, pp. 47–59 (in Russian).
7. Savishhenko N. V. *Pomexoustojchivost kogerentnogo priema mnogopozitsionnykh signalov KAM i FM pri neideal'noj sinxronizacii* [Interference immunity of coherent reception of multi-position QAM and FM signals with imperfect synchronization]. *Informacionno-upravlyayushhie sistemy*. 2010, no. 1, pp. 53–63 (in Russian).
8. Neguricza A. O. *Ocenka effektivnosti ispol'zovaniya Δ -sloya nerazlichimosti dvoichnykh signalov, prinimaemykh v usloviyax sluchajnykh i prednamerennykh pomex* [Assessment of the efficiency of using the Δ layer of indistinguishability of binary signals received in conditions of random and deliberate interference]. *Telekommunikacii i svyaz*, 2025, no. 4 (07), pp. 22–27 (in Russian).
9. Cahn C. Worst interference for coherent binary channel. *IEEE Transactions on Information Theory*, 1971, v. 17, no. 2, pp. 209–210. doi:10.1109/TIT.1971.1054597.
10. Vejcel' V. A., Zhodzishskij M. I., Zhodzishskij Yu. I. *Garantirovannaya pomexoustojchivost' priema signalov* [Worst interference for coherent binary channel]. *Radiotekhnika i elektronika*, 1987, v. 32, no. 2, pp. 316–321 (in Russian).
11. Bashar T., Wu Y.-W. A complete characterization of minimax and maximin encoder-decoder policies for communication channels with incomplete statistical description. *IEEE Transactions on Information Theory*, 1985, v. 31, no. 4, vpp. 482–489. doi:10.1109/TIT.1985.1057076.
12. Putilin A. N., Chudnov A. M. *Optimizatsiya priemnika fazomanipulirovannykh psevdosluchajnykh signalov pri naixudshej pomexe s ogranichennoj srednej moshhnost'yu* [Optimization of the receiver of phase-shift keyed pseudo-random signals at the worst interference with limited average power]. *Radiotekhnika i elektronika*, 1990, v. 35, no. 8, pp. 1646–1650 (in Russian).
13. Kullstam P. Spread spectrum performance analysis in arbitrary interference. *IEEE Transactions on Communications*, 1977, v. 25, no. 8, pp. 848–853. doi:10.1109/TCOM.1977.1093906.
14. Zhou S., Giannakis G. B., Swami A. Digital multi-carrier spread spectrum versus direct sequence spread spectrum for resistance to jamming and multipath. *IEEE Transactions on Communications*, 2002, v. 50, no. 4, pp. 643–655. doi:10.1109/26.996079.
15. Poisel R. A. Modern communications jamming: principles and techniques. Boston. Artech House, 2011.

16. Li S. Concise formulas for the area and volume of a hyperspherical cap. *Asian Journal of Mathematics and Statistics*, 2011, v. 4, no. 1, pp. 66–70. doi:10.3923/ajms.2011.66.70.

Статья поступила 03 марта 2026 г.

Информация об авторе

Негурица Анастасия Олеговна – соискатель ученой степени кандидата технических наук. Адъюнкт научно-исследовательского центра. Военная академия связи. Область научных интересов: помехоустойчивый прием и оценка качества передачи; геометрическое декодирование Хэмминга. Тел.: +7 966 715 90 67. E-mail: LadyN98@yandex.ru.

Адрес: Россия, 194064, г. Санкт-Петербург, Тихорецкий пр., д. 3.

Model for generating and receiving signals for analyzing and optimizing the noise immunity of a data transmission channel in the presence of intentional and random interference

A. O. Neguritsa

Annotation. Problem statement. It is required to build and investigate a model of receiving binary signals at the physical level of a communication channel under conditions of random noise and intentional interference, to obtain analytical dependencies of the probability of error for various interference modes, and to form a quality indicator reflecting the worst-case scenario with limited capabilities of the attacker. **The purpose of this work** is to obtain a guaranteed estimate of the bit error probability and to analyze the impact of the noise environment and the selected decision rule on the stability of the data transmission channel. **Methods used.** Statistical modeling at the level of decisive statistics after correlation (coordinated) processing, probabilistic analysis and derivation of analytical expressions for the probability of error, as well as the approach of guaranteed assessment of communication quality in the “worst-case violator” setting under resource constraints, are applied. **The novelty** consists in the joint consideration of non-coherent intentional interference and a randomized threshold decision rule for reception, as well as in the introduction of a guaranteed (worst-case) error probability as a metric for comparing reception options with a limited impact resource. **Result:** a discrete statistical channel model and analytical dependencies of the probability of error per bit for coherent and non-coherent interference modes have been obtained; a guaranteed reception quality assessment has been formed, which allows for a correct comparison of reception options and the study of the influence of interference parameters and the decision-making algorithm. **Practical significance:** the proposed model can be used for analytical assessment of the physical layer's noise immunity, justification of requirements for the communication channel's stability, and selection/configuration of receiving solutions when operating under conditions of combined random and intentional interference.

Keywords: data transmission channel, noise immunity, intentional interference, AWGN, coherent/incoherent reception, randomized decision rule for reception, bit error probability, guaranteed error probability, resource constraint.

Information about author

Anastasia Olegovna Neguritsa – Doctoral Student. The postgraduate student of the scientific research center. Field of research: noise-resistant reception and transmission quality assessment; geometric Hamming decoding. Tel.: +7 966 715 90 67. E-mail: LadyN98@yandex.ru.

Address: Russia, 194064, Saint-Petersburg, Tihoreckiy prospekt, 3.

Для цитирования:

Негурица А. О. Модель формирования и приема сигналов для анализа и оптимизации помехоустойчивости канала передачи данных в условиях преднамеренных и случайных помех // Техника средств связи. 2026. № 2 (174). С. 2-10. DOI: 10.24412/2782-2141-2026-2-2-10.

For citation:

Neguritsa A. O. Model for generating and receiving signals for analyzing and optimizing the noise immunity of a data transmission channel in the presence of intentional and random interference. *Means of Communication Equipment*, 2026, № 2 (174), Pp. 2-10 (in Russian). DOI: 10.24412/2782-2141-2026-2-2-10.

Развитие аппаратуры и систем связи на основе технологии когнитивного радио

Сулима А. А., Калямин И. В.

Аннотация. Постановка задачи: опыт участия в Сирийском конфликте, а также специальной военной операции на Украине показал необходимость проведения работ в части формирования единого информационного поля для управления воздушным эшелоном Вооруженных Сил Российской Федерации. В настоящее время профильными предприятиями активно ведутся работы по созданию унифицированного стека протокольных соглашений для информационного обмена в интересах управления и обеспечения связи, в том числе разнородных группировок войск. Однако реализация указанной концепции требует разработки алгоритмов распределения частотного ресурса и обеспечения устойчивости системы в целом ввиду возможного выбывания ее отдельных элементов. Решением указанных проблем является внедрение в системы связи и управления технологии когнитивного радио.

Целью работы является выбор наиболее оптимальной прогностической модели для построения когнитивной радиосистемы на основе последних принятых на вооружение образцов военной техники. Для анализа выбраны марковские и байесовские модели принятия решений, а также методы машинного обучения. **При моделировании используются методы** теории вероятности и математическое моделирование в программной среде Mathcad, Matlab. Предлагаемое решение предназначено к реализации в наиболее распространенных командных линиях управления диапазона 100 – 1600 МГц с его опциональным использованием в диапазонах 2 – 30 МГц и 2 – 6 ГГц. **Новизна обсуждаемого решения** состоит в интеграции прогностического модуля в состав аппаратуры управления систем связи, уже принятых на вооружение или разрабатываемых в настоящее время, в соответствии с изложенными в статье подходами. При этом решение накладывает аппаратные ограничения на используемые средства радиосвязи, которые должны использовать метод прямого цифрового преобразования сигнала, взамен широко внедренного супергетеродинного приема. **К результатам работы** на основе проведенного математического моделирования следует отнести выбор в качестве оптимальной прогностической модели (с учетом затрат на реализацию) для аппаратуры и систем связи воздушного эшелона управления байесовской модели с применением фильтра Калмана. **Практическая значимость работы** заключается в том, что при реализации концепции сетевцентричности в автоматизированных системах управления, предложенное решение позволяет повысить надежность всей системы с сохранением оперативности доведения информации за счет гибкой перестройки каналов связи между ее элементами еще до появления мешающего воздействия: работы средств радиоэлектронной борьбы, наличие естественных или промышленных помех, недостатка частотного ресурса в зоне работы, выбывания отдельных элементов системы и другое.

Ключевые слова: авиационные комплексы, когнитивное радио, средства связи, теория принятия решения.

Введение

Системы связи, представляющие собой оконечную приемопередающую аппаратуру, и радиоканалы между ними являются одним из важнейших элементов управления войсками. Наиболее остро вопрос оперативного доведения информации стоит для объектов воздушно-космических сил (ВКС), характеризующихся высокой скоростью перемещения, значительными расстояниями, сложной помеховой обстановкой, большим объемом информации, требуемым для принятия решений, скоростью передачи информации, необходимостью работы в разных диапазонах одновременно, высокой плотностью размещения радиосистем и поддержания функционирования разнообразных сетей. В связи с этим необходимо создание объединенной системы связи воздушного эшелона, включающей в себя современные радиосредства, обеспечивающие ее функционирование на высоком качественном уровне. Основными элементами, характеризующими системы связи, являются связность ее составляющих, имитоустойчивость, помехозащищенность, наращиваемость, устойчивость к выбыванию отдельных элементов [1].

При этом существующая система связи воздушного эшелона не удовлетворяет в полной мере ни одному из предъявляемых требований.

Постановка задачи

На сегодняшний день система управления и информационного обмена ВКС РФ состоит из разрозненных фрагментарных сегментов, строящихся вокруг стационарных пунктов управления, что препятствует построению устойчивой к выбыванию отдельных компонентов системы и единого информационного поля. Также аппаратура бортовых и наземных комплексов связи часто использует несовместимые между собой стандарты, зачастую устаревшие и не отвечающие современным требованиям по помехозащите, помехоустойчивости, скорости и надежности передачи информации. При этом построение комплексов связи на основе устаревших аппаратных решений не позволяет проводить их оперативную модернизацию с целью интеграции в единое информационное поле вооруженных сил (ВС) РФ. Отсутствие единого подхода приводит к тому, что вновь разрабатываемые комплексы и системы связи не являются в полной мере взаимосовместимыми и часто позволяют работать встречно со всем парком аппаратуры только в режиме амплитудной модуляции (открытая телефонная связь) со всеми вытекающими из этого ограничениями.

В то же время в странах потенциальных партнеров реализуются системные подходы (например, программа *STANAG*) к проектированию информационных систем и аппаратуры связи. Это позволяет оперативно включать в единый контур различные типы летательных аппаратов, в том числе беспилотные (БЛА). При этом возможна работа не только с пунктами управления разного ранга и территориального расположения, но и в смешанных группах летательных аппаратов с целью использования их преимуществ. Примерами таких системных подходов могут являться программы *JTRS* и *Link-16*. Соответственно, для сохранения научно-технического и военного паритета перспективные системы воздушного эшелона ВКС РФ и составляющая их аппаратура должны позволять реализовывать наиболее передовые технические решения, позволяющие решать существующие задачи, и иметь значительный потенциал модернизации и наращивания функционала.

Для удержания паритета необходимо решить вопрос эффективного использования радиочастотного спектра. Причем если в гражданской сфере это достигается лицензированием используемых частот, организацией пространственного разнесения высокомошных передатчиков (например, базовых станций) и другими, достаточно простыми методами, то в военной сфере, при ведении боевых действий (активном радиоэлектронном противодействии противника и значительном количестве работающих передающих систем), подобные методы не применимы.

В настоящее время, в военных системах радиосвязи используются различные методы повышения помехозащищенности радиоканала, автоматизированное составление планов связи для летательных аппаратов, а также изменение вручную режимов работы радиосредств при ухудшении качества приема. Однако подобные решения требуют участия человека в той или иной форме, что неприменимо в беспилотной боевой авиации, получившей распространение в последние годы, да и в целом подобные технические решения идеологически не пригодны для самолетов нового поколения (в частности, самолета Су-75 *Checkmate*), где требуется максимально возможная автоматизация выполняемых процессов [2].

Кроме того, все чаще тактика применения средних и малых БЛА заключается в их групповом использовании (в том числе и с элементами самоорганизации), при этом эффективность группы зависит от эффективности внутригруппового взаимодействия между БЛА и функционирования командных радиолиний в целом. Эффективность же данного взаимодействия, в свою очередь, зависит от эффективности (скорости, надежности, помехозащищенности) систем связи БЛА. При этом классические методы обеспечения связи

уязвимы для систем радиоэлектронной борьбы противника, как из-за отсутствия пилота, способного принимать решения об изменении плана связи, так и из-за ограниченности частотного диапазона, используемого БЛА. Наиболее простым и одновременно наименее эффективным путем является адаптация системы связи к изменяющемуся состоянию помеховой обстановки. Это технические решения, предусматривающие автоматическое управление параметрами передатчика (изменение мощности, дублирование, адаптивная смена частоты и т. д.). Однако учитывая, что в большинстве случаев адаптация происходит уже после обнаружения мешающего воздействия, то неизбежны потери информации, а также в некоторых случаях проявляется неэффективность адаптации.

Таким образом, особую актуальность приобретает задача реализации в системах связи когнитивных режимов работы. Причем предлагаемое решение должно быть подходящим для различных типов летательных аппаратов и условий базирования, а также обладать свойством масштабируемости, простотой интеграции и возможностью оперативной модернизации.

Метод решения

Одним из вариантов решения данной задачи является переход на системы когнитивного радио (*CRS*) для оснащения летательных аппаратов. Внедрение систем на основе технологии когнитивного радио требует решения вопросов по созданию аппаратной платформы и алгоритмов ее функционирования. Одной из наиболее важных задач для *CRS* является разработка алгоритма оценки и выбора наиболее эффективного (с точки зрения помеховой обстановки, пропускной способности, «загруженности») радиоканала и используемой сигнально-кодовой конструкции. К особенностям радиосвязных систем на основе когнитивного радио можно отнести:

- возможность получения информации из радиоканала и от вспомогательных бортовых систем;
- возможность проводить интеллектуальный анализ полученной информации;
- изменять параметры радиосистемы при изменении состояния помеховой обстановки для обеспечения наиболее эффективного функционирования радиосистемы.

Комплекс, построенный на основе *CRS*, должен не просто определять наиболее оптимальный частотный ресурс для связи, но и прогнозировать его изменение в перспективе в конкретный момент времени с учетом возможного противодействия или резкого ухудшения помеховой обстановки. При этом в состав когнитивной радиосистемы должны входить:

- система анализа состояния радиоэфира – сверхширокополосный приемник, принимающий, оцифровывающий и анализирующий всю полосу приема и выделяющий полезные сигналы, мешающие помехи и общее состояние радиоэфира в обслуживаемой полосе;
- система принятия решений с прогностическим модулем, представляющая собой программное обеспечение, установленное на специализированный вычислитель;
- база данных, обновляемая по мере получения информации от различных источников;
- алгоритм связи с абонентами группы (программное обеспечение (ПО), осуществляющее выбор наиболее оптимального радиоканала);
- собственно сама радиостанция (приемник и передатчик информации, модем, усилители мощности).

В приближенном виде в качестве платформы для построения когнитивной радиосистемы возможно использовать радиосвязную платформу самолета 5-го поколения Су-57, которая включает в свой состав многофункциональный вычислитель со специализированным ПО, работающим под управлением операционной системы реального времени (ОС РВ), и широкодиапазонный модуль связи, позволяющий обеспечивать анализ всей полосы частот в диапазоне 2 – 520 МГц и использовать различные типы сигнально-кодовых конструкций. Общая структурная схема когнитивной радиосистемы представлена на рис. 1.

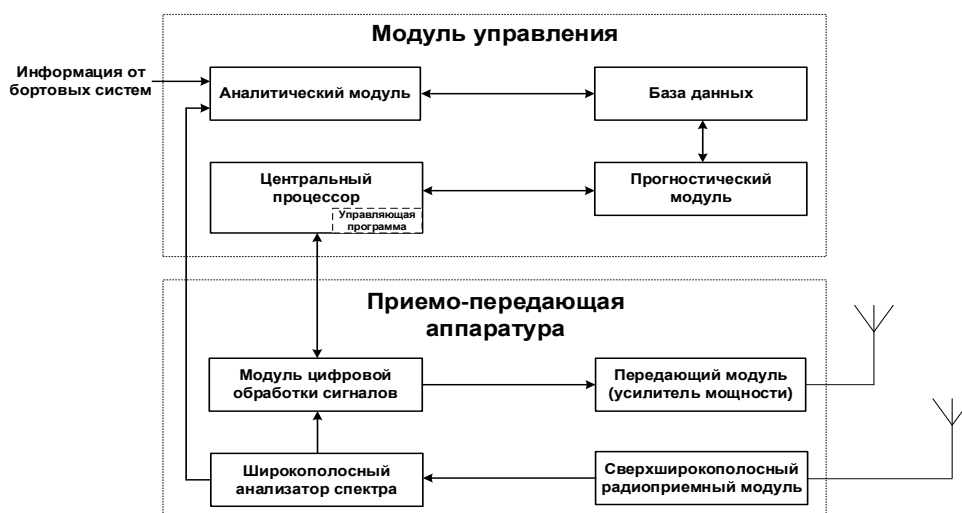


Рис. 1. Общая структурная схема когнитивной радиосистемы

На рис. 1 видно, что анализатор спектра, приемное, передающее устройство и модуль цифровой обработки сигнала объединены в одно устройство, а хранилище базы данных, устройство управления и аппаратура, обеспечивающая работу с прогностической моделью, в другое [3].

Критерием качества канала, в дальнейшем планируемого под использование для передачи информации, является оценка уровня шума в радиоканале, а также количество правильно принятых сообщений (оценивается вероятность битовой ошибки), при этом битовая ошибка имеет больший весовой коэффициент для принятия решения аналитической системой. Добавочным показателем качества канала и оценки возможности его использования для передачи информации являются задачи/планы связи (т. е. информация о заранее зарезервированных частотах для использования в качестве рабочих другими абонентами, находящимися в данном районе), частота появления и длительность нахождения других абонентов на предпочтительных частотах, а также прогноз состояния каналов связи на основе полученных данных за определенный период времени.

Очевидно, что одним из основных требований к приемной системе когнитивного радио должна являться возможность прослушивания (мониторинга) нескольких частот/каналов (требует построения CRS на основе приемников прямой обработки сигнала), с последующим анализом радиоэфира на наличие полезного сигнала, его качества, и в дальнейшем информационного содержания, при этом сравнивается сигнатура полученных сигналов с базой данных, возможных к использованию системой БЛА, на основании чего, информация о состоянии радиоэфира вносится в базу данных, при этом каждому оцениваемому параметру присваивается свой весовой коэффициент, в частности важную роль играет тип обнаруженного сигнала, это может быть:

- полезный сигнал, используемый абонентами в группе (совпадает сигнатура прослушанного сигнала с сигнатурами в базе данных и используемая служебно-адресная часть в сообщении);
- сигнал, определяемый как не относящийся к категории «своих» (определяется наличие сигнала, но не определяется информационное содержимое);
- искусственная помеха;
- естественный шум.

Одновременно база данных обновляется информацией, получаемой от других БЛА (при наличии канала связи), поскольку в обмене участвует сразу несколько абонентов и должно учитываться состояние радиоэфира на других участках сети, информация о которых передается в содержательной части передаваемых сообщений (передается информация о наиболее энергетически выгодных каналах определенного абонента). Получив

данную информацию, аналитический модуль обновляет базу данных о состоянии радиоканалов. Прогностический модуль формирует модель состояния каналов радиосвязи в тот или иной промежуток времени, и в соответствии с ней выбирает наиболее подходящий на ближайший период времени план связи. При этом в плане связи формируется таблица каналов, обеспечивающих с допустимой вероятностью передачу информации с заданной надежностью/достоверностью. Каждому из этих каналов присваивается свой коэффициент предпочтительности, при этом радиоприемное средство настраивается на прием на все прогнозируемые каналы (например, современные радиосредства 5-го поколения, такие как комплекс средств связи С-111 обеспечивает одновременный прием до 200 каналов в одном диапазоне). После настройки радиосредства и выбора оптимальных частот, начинается передача тестовых сообщений с использованием таблицы наиболее оптимальных/вероятных каналов (от самого вероятного к наименее вероятному) до момента получения подтверждающего сообщения (фактически происходит использование режима автоматического установления связи *ALE*) или квитанции от абонента. После получения ответного сообщения радиосистема остается на используемом канале до тех пор, пока вероятность битовой ошибки не начнет превышать заданную, либо измеряемое соотношение сигнал/шум выйдет за допустимые границы. Сама система в процессе ведения радиосвязи продолжает анализировать помеховую обстановку с целью поддержания базы данных в актуальном состоянии, благодаря чему в любой момент времени существует список наиболее оптимальных для связи частот, информация о которых также передается абонентам группы, для обновления имеющихся на них баз данных. В перспективе, база данных для формирования и прогноза может быть привязана не только к параметрам канала, но и высоте полета, местоположению, а также ряду других данных, получаемых от систем БЛА или наземных служб (пунктов управления). Кроме того, возможно введение таких дополнительных параметров, как скорость передачи информации и используемые помехоустойчивые коды.

Необходимо отметить, что подобная прогностическая модель должна предугадывать оптимальные каналы с высокой вероятностью, в противном случае применение когнитивных систем в интересах вооруженных сил становится неоптимальным, как с точки зрения скорости установления каналов, так и радиозаметности БЛА. При этом в случае неверного или неоптимального прогноза придется выходить на передачу на множестве частот, тем самым обнаруживая себя и дискредитируя используемые каналы (частоты) связи. В случае же удачно выбранной прогностической модели и верного распределения вероятности формирования каналов связи возможна не только устойчивая связь на определенном канале, но и его оперативная смена в соответствии с меняющейся обстановкой. В любом случае рассмотренная система в разы эффективнее существующих, где решения принимаются очень инерционно, требуют участия человека, а в случае разрыва канала управления – отсутствует возможность быстрого подбора необходимого частотного плана [4].

Существует несколько типов интеллектуальных моделей предсказания изменения параметров, представляющихся перспективными для использования в прогностическом модуле систем связи:

- марковские цепи / скрытые марковские модели [5-9]. Используются для прогнозирования состояния канала, представляя его в виде последовательности дискретных состояний с заданными вероятностями переходов. Хотя этот подход наиболее изучен, часто он требует упрощающих предположений о свойствах канала и может быть неэффективен для моделирования сложных зависимостей между множеством факторов. С другой стороны, в случае работы по упрощенной модели канала или по небольшому числу параметров данный подход является перспективным техническим направлением;
- модели машинного обучения на основе ансамблей деревьев решений (*Random Forest*) и градиентного бустинга (*XGBoost*) [10, 11]. В последние годы активно

исследуется применение глубоких нейронных сетей и их обучение для управления ресурсами в беспроводных сетях. Эти методы показывают высокую эффективность, но зачастую требуют значительных вычислительных ресурсов, больших объемов данных для обучения и могут являться «черным ящиком» для разработчика, что не всегда приемлемо при сертификации критически важных систем связи;

- байесовская модель с применением фильтра Калмана [12-14]. Является хорошо зарекомендовавшим себя математическим аппаратом. Подходит для моделирования сложных вероятностных зависимостей между множеством факторов (уровень помех, уровень сигнала, время суток, активность пользователей и т. д.) и принятия решений в условиях неопределенности. Фильтр Калмана в свою очередь является оптимальным инструментом для оценки и прогнозирования непрерывно меняющихся параметров динамической системы в условиях шумов.

В качестве объекта для возможного внедрения и проведения исследований был выбран комплекс средств связи С-111, обеспечивающий режимы группового взаимодействия в телекодовых сетях (ТКС) диапазона 100 – 400 МГц. Принятые в ТКС системные соглашения доказали свою состоятельность в процессе испытаний в части информационного обмена разнородных объектов, что привело к их широкому внедрению в войсках. Проведенное моделирование показало, что наиболее эффективно использовать последний из предложенных методов, при этом эффективность оценивалась с точки зрения скорости проведения прогностических расчетов, точности предсказания моделей и затрат на реализацию (рис. 2).

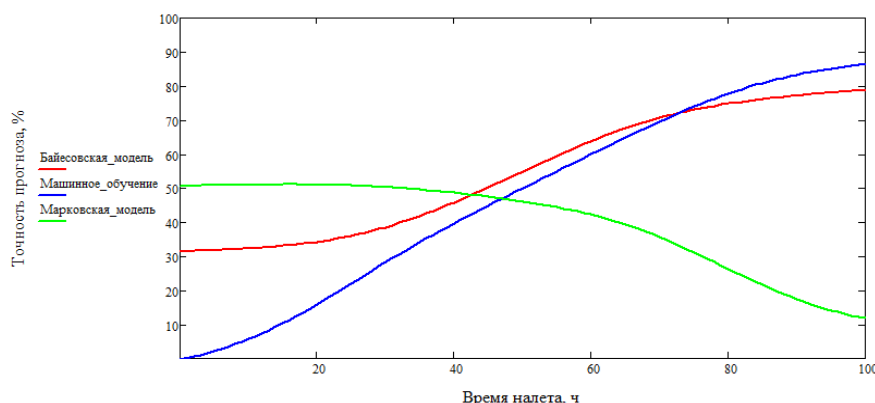


Рис. 2. Эффективность прогностических моделей для информационной сети (16 абонентов) в условиях радиоэлектронного противодействия и изменяющейся топологии сети

Для создания наиболее эффективной когнитивной радиосистемы должны быть решены следующие научно-технические задачи:

- разработка регламентирующих документов в части организации каналов связи;
- расширение рабочего диапазона комплексов радиосвязи;
- создание алгоритмов функционирования систем радиосвязи на основе самоорганизующихся сетей;
- создание единой концепции передачи данных в разных диапазонах;
- разработка интеллектуальных систем управления и специализированных экспертных систем принятия решений на основе элементов искусственного интеллекта;
- переход на архитектуру программно-определяемого радио (SDR) (система радиосвязи, использующая технологию программной реализации режимов работы для компонентов системы радиосвязи).

В идеале, когнитивная радиостанция будет представлять собой изделие, обрабатывающее широкую полосу сигналов с одновременным анализом состояния радиозфира, предсказывать его изменение на ожидаемом промежутке времени и определять

наиболее эффективные режимы работы, что позволит обеспечивать оперативный (адаптивный) выбор наиболее оптимальных режимов работы, каналов, видов модуляции.

При передаче сообщений по радиоканалам параметры передаваемых сигналов определяются из условия обеспечения требуемой достоверности, энергетической эффективности и наиболее эффективного коллективного распределения частотного ресурса. В условиях изменяющегося состояния канала (в том числе по причине радиоэлектронного противодействия) можно приблизиться к теоретически возможной пропускной способности канала связи для заданного числа абонентов в сети за счет построения интеллектуальной (когнитивной) системы радиосвязи.

Задача когнитивного управления системами связи на сетевом уровне, затрагивающем несколько абонентов, одновременно работающих в одной зоне и использующих каналы с динамически изменяющимися параметрами, является сложной задачей, зачастую с многими неизвестными. Кроме того, принятие решений на сетевом уровне зависит от специфики передаваемой информации, ранга абонента, возможности ретрансляции и объема сформированной базы состояния радиоэфира. Дополнительное повышение эффективности передачи информации может быть достигнуто за счет управления информационными потоками с учетом содержания передаваемых сообщений [15].

Фактически в данном случае формируется распределенная интеллектуальная система воздушно-наземной связи (ИСВНС) – информационное пространство между разнесенными по территории страны объектами, объединенными едиными задачами, и ресурсами интеллектуальной сети, управляемыми по определенным алгоритмам для всех летательных аппаратов воздушного эшелона, в который входят: дальняя, военно-транспортная, оперативно-тактическая и армейская авиация, беспилотные летательные аппараты, специальная авиация, представленная объектами системы воздушных пунктов управления, и авиация военно-морского флота, а так же имеются каналы связи с различными системами космического, наземного и морского эшелонов.

Процесс функционирования ИСВНС необходимо организовать таким образом, чтобы создать самообучающуюся систему, непрерывно отслеживающую занятость частотного ресурса, потребности пользователей и управляющую в реальном масштабе времени радиосвязным оборудованием, распределяя ресурс в соответствии с установленными принципами и приоритетами.

Выводы

Создание систем на основе технологии *CRS* (как на аппаратном, так и сетевом уровнях) обеспечит значительное улучшение возможностей по управлению и координации действий объектов ВС РФ, своевременному и надежному доведению до каждого участника военной операции информации, необходимой для решения общей боевой задачи.

Таким образом, учитывая динамично изменяющиеся условия современных войн, создание аппаратуры, поддерживающей технологию *CRS* даже в самом упрощенном виде, является наиболее приоритетной задачей для профильных организаций. При этом простые в освоении и реализации Байесовские модели также могут использоваться в построении подобных систем, показывая определенные преимущества перед нейронными сетями.

Литература

1. Сулима А. А. Способ повышения помехозащищенности перспективных систем воздушной радиосвязи с использованием фазированных антенных решеток и алгоритмов адаптивного построения каналов // Радиотехнические и телекоммуникационные системы. 2023. № 1. С. 41-49. DOI: 10.24412/2221-2574-2023-1-41-49.

2. Патент на изобретение № 2762743 РФ, МПК H04B 7/00. Комплекс бортовых средств цифровой радиосвязи: № 2020134531: заявл. 20.10.2020: опубл. 22.12.2021 / Комяков А. В., Войткевич К. Л., Сулима А. А., Колобков А. В.; заявитель АО «НПП «Полет». – 11 с.
3. Патент на изобретение № 2780716 РФ, МПК F41G 3/22. Система управления вооружением летательных аппаратов: № 202111918: заявл. 29.06.2021: опубл. 29.09.2022 / Большаков С. Б., Войткевич К. Л., Комяков А. В. [и др.]; заявитель АО «НПП «Полет». – 36 с.
4. Yonina C. Eldar, Andrea Goldsmith, Deniz Gündüz, and H. Vincent Poor. Machine Learning and wireless communication // Cambridge University Press. 2023.
5. Abir Ray. Scalable Spectrum Availability Prediction using a Markov Chain Framework and ITU-R Propagation Models. Cornell University, Systems Engineering, Ithaca, NY USA. 2025. – URL: <https://arxiv.org/abs/2508.00028> (дата обращения 20.02.2026).
6. Corlay V., Nakazato T., Yamaguchi K., Nakajima A. Differentiable High-Order Markov Models for Spectrum Prediction // IEEE International Conference on Machine Learning for Communication and Networking (ICMLCN). 2024. – URL: <https://arxiv.org/html/2412.00328v1> (дата обращения: 20.02.2026).
7. Omer A. S., Tufa A. D., Debella T. T., Woldegebreal D. H. Hidden Markov Models for Predicting Cell-Level Mobile Networks Performance Degradation // e-Prime – Advances in Electrical Engineering Electronics and Energy. 2024. Vol. 9.
8. Hirsch C., Bharti A., Pedersen T., Waagepetersen R. Bayesian Inference for Stochastic Multipath Radio Channel Models // IEEE Transactions on Antennas and Propagation. 2023, v. 71, no. 4, pp. 3460-3472.
9. Сопин Э. С., Маслов А. Р. Об аппроксимация вероятности прерывания сессии в беспроводных сетях миллиметрового диапазона частот // XIV Всероссийское совещание по проблемам управления : сборник научных трудов, Москва, 17–20 июня 2024 года. Москва: Институт проблем управления им. В.А. Трапезникова РАН. 2024. С. 2326-2329.
10. Аверина Л. И., Беликов Д. И. Прогнозирование состояния сигнально-помеховой обстановки на основе машинного обучения // Теория и техника радиосвязи. 2024. № 2. С. 5-12.
11. Брагин К. И., Норицин И. А., Дроздова В. Г. Имитационная модель для исследования алгоритмов планирования радиоресурсов уровня доступа в сетях мобильной связи // Труды учебных заведений связи. 2025. Т. 11. № 5. С. 84-96. DOI: 10.31854/1813-324X-2025-11-5-84-96.
12. Szczecinski L, Benesty J, Kuhn E. V. A unified Bayesian perspective for conventional and robust adaptive filters // Signal Processin. 2026. Vol. 238.
13. Шахтарин Б. И. Фильтры Винера и Калмана: учебное пособие. М.: Горячая линия – Телеком, 2024. – 396 с.
14. Salari S., Chan F. Joint CFO and Channel Estimation in OFDM Systems Using Sparse Bayesian Learning // IEEE Communication Letters. 2021, v. 25, no. 1, pp. 166-170.
15. Сулима А. А. Методы повышения помехозащищенности комплексов воздушной связи // Телекоммуникации и связь. 2025. № 6. С. 51-57. DOI: 10.21681/3034-4050-2025-6-51-57.

References

1. Sulima A.A. *Sposob povysheniya pomekhozashchishchennosti perspektivnykh sistem vozdushnoy radiosvyazi s ispol'zovaniyem fazirovannykh antennoykh reshetok i algoritmov adaptivnogo postroyeniya kanalov* [A Method for Improving the Noise Immunity of Advanced Airborne Radio Communication Systems Using Phased Antenna Arrays and Adaptive Channel Construction Algorithms]. *Radio Engineering and Telecommunication Systems*, 2023, no. 1, pp. 41-49 (in Russian).
2. Patent for invention no. 2762743 of the Russian Federation, IPC H04B 7/00. *Kompleks bortovykh sredstv tsifrovoy radiosvyazi* [Complex of on-board digital radio communication equipment]. No. 2020134531, application 10.20.2020, publ. 12.22.2021. Komyakov A. V., Voytkevich K. L., Sulima A.A., Kolobkov A. V., applicant JSC “POLYOT Research & Production Company”, 11 p. (in Russian).
3. Patent for invention no. 2780716 of the Russian Federation, IPC F41G 3/22. *Sistema upravleniya vooruzheniyem letatel'nykh apparatov* [Aircraft weapons control system]. No. 202111918, application 06.29.2021, publ. 09.29.2022. Bolshakov S. B., Voitkevich K. L., Komyakov A. V. [et al.], applicant JSC “POLYOT Research & Production Company”, 36 p. (in Russian).

4. Eldar Y. C., Goldsmith A., Gündüz D., Poor H. V. Machine Learning and Wireless Communication. Cambridge. Cambridge University Press. 2023.
5. Ray A. Scalable Spectrum Availability Prediction using a Markov Chain Framework and ITU-R Propagation Models. Cornell University, Systems Engineering, Ithaca, NY USA. 2025. Available at: <https://arxiv.org/abs/2508.00028> (accessed 20 February 2026).
6. Corlay V., Nakazato T., Yamaguchi K., Nakajima A. Differentiable High-Order Markov Models for Spectrum Prediction. IEEE International Conference on Machine Learning for Communication and Networking (ICMLCN). 2024. Available at: <https://arxiv.org/html/2412.00328v1> (accessed 20 February 2026).
7. Omer A. S., Tufa A. D., Debella T. T., Woldegebreal D. H. Hidden Markov Models for Predicting Cell-Level Mobile Networks Performance Degradation. e-Prime – Advances in Electrical Engineering Electronics and Energy. 2024, v. 9.
8. Hirsch C., Bharti A., Pedersen T., Waagepetersen R. Bayesian Inference for Stochastic Multipath Radio Channel Models. IEEE Transactions on Antennas and Propagation. 2023, v. 71, no. 4, pp. 3460-3472.
9. Sopin E. S., Maslov A. R. *Ob approximationsiya veroyatnosti preryvaniya sessii v besprovodnykh setyakh millimetrovogo diapazona chastot* [On the approximation of the probability of session interruption in millimeter-wave wireless networks]. XIV All-Russian Conference on Control Problems: collection of scientific papers, Moscow, June 17–20, 2024. Moscow: V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences. 2024. Pp. 2326–2329 (in Russian).
10. Averina L. I., Belikov D. I. *Prognozirovaniye sostoyaniya signal'no-pomekhovoy obstanovki na osnove mashinnogo obucheniya* [Forecasting the state of the signal-interference environment based on machine learning]. *Theory and technology of radio communication*, 2024, no. 2, pp. 5-12 (in Russian).
11. Bragin K. I., Noritsin I. A., Drozdova V. G. *Imitatsionnaya model' dlya issledovaniya algoritmov planirovaniya radioresursov urovnya dostupa v setyakh mobil'noy svyazi* [Simulation model for studying algorithms for planning radio resources of the access level in mobile communication networks]. *Proceedings of educational institutions of communication*, 2025, v. 11, no. 5, pp. 84-96 (in Russian).
12. Szczecinski L, Benesty J, Kuhn E. V. A unified Bayesian perspective for conventional and robust adaptive filters. *Signal Processin.* 2026, v. 238.
13. Shakhtarin B. I. *Fil'try Vinera i Kalmana* [Wiener and Kalman Filters]. Moscow. Goryachaya Liniya-Telecom, 2024, 396 p. (in Russian).
14. Salari S., Chan F. Joint CFO and Channel Estimation in OFDM Systems Using Sparse Bayesian Learning. *IEEE Communication Letters*, 2021, v. 25, no. 1, pp. 166-170.
15. Sulima A. A. *Metody povysheniya pomekhozashchishchennosti kompleksov vozdukhnoy svyazi* [Methods for improving the interference immunity of airborne communication systems]. *Telecommunications and Communications*, 2025, no. 6, pp. 51-57 (in Russian).

Статья поступила 24 февраля 2026 г.

Информация об авторах

Сулима Алексей Александрович – заместитель начальника научно-технического центра штатных комплексов средств связи летательных аппаратов. Акционерное общество «Научно-производственное предприятие «Полет». Область научных интересов: проектирование и разработка когнитивных радиосистем. Тел.: +7(831)244-87-41. E-mail: radio@npp-polyot.ru.

Калямин Илья Викторович – начальник отдела перспективных комплексов средств связи летательных аппаратов. Акционерное общество «Научно-производственное предприятие «Полет». Область научных интересов: проектирование и разработка когнитивных радиосистем. Тел.: +7(831)244-87-41. E-mail: otd3060@npp-polyot.ru.

Адрес: Россия, 603950, г. Нижний Новгород, Комсомольская пл., д. 1.

Development of communication equipment and systems based on cognitive radio technology

A. A. Sulima, I. V. Kalyamin

Annotation. Task statement: the experience of participation in the Syrian conflict, as well as a special military operation in Ukraine, showed the need for work in terms of forming a single information field for controlling the air echelon of the Armed Forces of the Russian Federation. Currently, specialized enterprises are actively working to create a unified stack of protocol agreements for information exchange in the interests of management and communication, including heterogeneous groupings of troops. However, the implementation of this concept requires the development of algorithms for allocating frequency resource and ensuring the stability of the system as a whole due to the possible elimination of its individual elements. The solution to these problems is the introduction of cognitive radio technology into communication and control systems. **The purpose of the work** is to select the most optimal predictive model for building a cognitive radio system based on the latest adopted samples of military equipment. Markov and Bayesian decision models, as well as machine learning methods were selected for the analysis. Modeling uses methods of probability theory and mathematical modeling in the Mathcad software environment, Matlab. The proposed solution is designed to be implemented in the most common control command lines of the 100-1600 MHz band with its optional use in the 2-30 MHz and 2-6 GHz bands. **The novelty** of the discussed solution is the integration of the prognostic module into the control equipment of communication systems already adopted or currently being developed, in accordance with the approaches described in the article. At the same time, the solution imposes hardware restrictions on the used radio communication means, which must use the method of direct digital signal conversion, instead of the widely implemented superheterodyne reception. **The results of work** based on mathematical modeling should include the choice as the optimal prognostic model (taking into account the cost of implementation) for equipment and communication systems of the air control level of the Bayesian model using the Kalman filter. **The practical significance of the work** lies in the fact that when implementing the concept of network centrality in automated control systems, the proposed solution makes it possible to increase the reliability of the entire system while maintaining the efficiency of information delivery due to the flexible adjustment of communication channels between its elements even before the appearance of an interfering effect: operation of electronic warfare equipment, presence of natural or industrial interference, lack of frequency resource in the area of operation, elimination of individual elements of the system, etc.

Keywords: aviation complexes, cognitive radio, communications, decision theory.

Information about the authors

Alexey Alexandrovich Sulima – Deputy Head of the Scientific and Technical Center of the staff complexes of aircraft communications. Joint Stock Company "Scientific and Production Enterprise "Flight." Research interests: design and development of cognitive radio systems. Tel.: +7 (831) 244-87-41. E-mail: radio@npp-polyot.ru.

Ilya Viktorovich Kalyamin – Head of the Department of Advanced Communication Complexes of Aircraft. Joint Stock Company "Scientific and Production Enterprise "Flight." Research interests: design and development of cognitive radio systems. Tel.: +7 (831) 244-87-41. E-mail: otd3060@npp-polyot.ru.

Address: Russia, 603950, Nizhny Novgorod, Komsomolskaya square, 1.

Для цитирования:

Сулима А. А., Калямин И. В. Развитие аппаратуры и систем связи на основе технологии когнитивного радио // Техника средств связи. 2026. № 2 (174). С. 11-20. DOI: 10.24412/2782-2141-2026-2-11-20.

For citation:

Sulima A. A., Kalyamin I. V. Development of communication equipment and systems based on cognitive radio technology. *Means of Communication Equipment*, 2026, no. 2 (174), pp. 11-20 (in Russian). DOI: 10.24412/2782-2141-2026-2-11-20.

ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 004.056

DOI: 10.24412/2782-2141-2026-2-21-30

Метод оценки защищенности информации и информационной безопасности объекта критической информационной инфраструктуры

Фаткиева Р. Р., Билятдинов К. З., Фортинский А. Г.

Аннотация. *Постановка задачи:* функционирование объектов критической информационной инфраструктуры в современных условиях характеризуется увеличением числа угроз. В этой связи возрастает необходимость оценки уровня защищенности информации в них. Возникает проблема перехода от периодического к непрерывному мониторингу состояния безопасности обработки и передачи информации. Однако в настоящее время модели и методы, позволяющие формализованно учитывать динамику изменения показателей информационной безопасности, остаются недостаточно проработанными, что ограничивает возможность своевременного выявления нарушений безопасности. **Целью работы** является разработка научно-методического аппарата интегральной оценки защищенности информации на основе совокупности частных показателей с учетом их значимости. **Используемые методы:** исследование выполнено с применением методов системного анализа, многокритериальной оценки уровней защищенности, анализа уязвимостей и угроз, сценарного моделирования нарушений. **Результат:** разработан метод количественной оценки защищенности информации и информационной безопасности объекта критической информационной инфраструктуры. **Новизна** состоит в том, что предложенная интегральная оценка защищенности информации учитывает динамику изменения частных показателей во времени и формализованно агрегирует количественные показатели с учетом их значимости. Разбиение показателей на группы позволяет в случае необходимости расширить их состав. Это обеспечивает более точное отражение реального состояния защищенности информации анализируемого объекта и позволяет своевременно выявлять деструктивные воздействия. **Практическая значимость** предложенного подхода может использоваться для поддержки управленческих решений, планирования мероприятий по защите информации и сравнения уровня защищенности различных объектов критической инфраструктуры. Полученные результаты в дальнейшем могут быть использованы для количественной оценки и мониторинга других параметров сложных технических систем.

Ключевые слова: интегральная оценка, информационная безопасность, объект критической информационной инфраструктуры, многокритериальная оценка, оценка рисков информационной безопасности, показатель защищенности информации, частные показатели.

Актуальность

В современном мире объекты критической информационной инфраструктуры (ОКИИ) играют ключевую роль в обеспечении жизнедеятельности общества и функционировании государства, поскольку охватывают широкий спектр объектов и являются жизненно важными для обеспечения национальной безопасности и стабильного развития экономики. Учитывая растущие угрозы со стороны кибернарушений, обеспечение безопасности ОКИИ становится приоритетной задачей для обеспечения информационной безопасности (ИБ) в стране.

В этих условиях одной из ключевых задач является оценка текущего состояния защищенности информации, которая необходима для обоснования выбора мероприятий защиты, и контроля эффективности их выполнения. Анализ существующих методологических подходов к оценке ИБ в ОКИИ показывает, что большая часть из них ориентирована на экспертные оценки [1-3]. Отдельные нормативно-правовые акты и исследования [4] используют фиксированные наборы показателей и уровней защищенности, привязанные к

конкретным классам или категориям значимости ОКИИ, что затрудняет адаптацию множества показателей при изменении их состава, перестроении модели угроз, или необходимости корректировки показателей согласно изменениям в требованиях регуляторов.

Зачастую разработанные методы построения системы показателей ИБ корректно отражают степень защищенности только в рамках конкретного ОКИИ, что затрудняет сопоставление уровней защищенности между различными типами ОКИИ. Это ограничивает возможность использования методов для анализа эффективности принимаемых мер и принятия управленческих решений на уровне отрасли. Разработанные методы [5-8], как правило, рассматривают частные показатели как независимые, без учета их корреляции, что приводит к дублированию показателей, замедлению времени реакции на то или иное нарушение и как следствие неправильную оценку интегрального показателя защищенности.

Представленные в [9, 10] системы показателей защищенности в своем большинстве ориентировано на фиксацию значений частных показателей в дискретные моменты времени и не предусматривают непрерывный мониторинг динамики их изменения. Это приводит к тому, что кратковременные нарушения требований ИБ могут быть пропущены в итоговой интегральной оценке защищенности в процессе агрегирования. Вялотекущие тенденции ухудшения состояния ОКИИ могут быть не зафиксированы отдельными показателями, что может привести к сглаживанию негативных изменений и снижению чувствительности интегрального показателя к реальным инцидентам, а это в свою очередь, ограничивает идентификацию угроз. Также недостаточная чувствительность интегральной оценки к изменениям частных показателей снижает обоснованность принимаемых решений в области обеспечения ИБ и, как следствие, приводит к нерациональному распределению ресурсов, в частности избыточных мер защиты в одних направлениях при недостаточном уровне внимания к критически важным компонентам системы безопасности в других.

Таким образом, отсутствие учета динамики показателей требует необходимости перехода к непрерывному мониторингу состояния защищенности информации. В связи с этим разработка методологических основ динамической оценки защищенности информации позволит повысить ее объективность и воспроизводимость, а также обеспечить разработку теоретических основ для поддержки процессов управления ИБ в рамках требований нормативно-правовых документов Российской Федерации.

Постановка задачи

Пусть задано конечное множество показателей защищенности, в котором каждый показатель характеризует отдельное состояние безопасности информации в ОКИИ, с возможностью количественной или качественной оценки. Требуется разработать метод оценки защищенности информации в ОКИИ на базе интегральной оценки показателей, с учетом их значимости. Разрабатываемый метод должен удовлетворять ограничениям и требованиям решаемой задачи: быть применимым для различных типов ОКИИ; быть независимым от фиксированного числа уровней показателей защищенности; допускать расширение состава показателей, а также структуры их агрегирования без изменения типа интегрального показателя.

Метод оценки защищенности информации и информационной безопасности объекта критической информационной инфраструктуры

Метод оценки показателя состояния технической защиты информации включает следующие этапы:

Шаг 1. Сбор исходных данных, необходимых для формирования системы показателей защищенности анализируемого ОКИИ, для этого осуществляется:

1.1 Анализ этапов функционирования ОКИИ. Исходными данными, необходимыми для формирования системы показателей защищенности являются: внутренние организационно-

распорядительные документы, регламентирующие организацию защиты информации; эксплуатационная документация на средства защиты информации (СЗИ), содержащая сведения об их настройках и конфигурации; результаты проведения инвентаризации информационной системы (ИС), автоматизированной системы управления (АСУ), информационно-телекоммуникационной системы (ИТКС); результаты анализа функционирования отдельных программных, программно-аппаратных средств, сетевой инфраструктуры организации и мониторинга ИБ. В случае необходимости осуществляется опрос сотрудников организации о составе и порядке реализации ими задач при обеспечении ИБ.

1.2 Формирование конечного множества показателей защищенности технических средств защиты ОКИИ (рис. 1):

$$X^l = \{x_1^l, x_2^l, \dots, x_i^l, \dots, x_{N_l}^l\}, i = \overline{1, N_l}, \quad (1)$$

где x_i^l – i -ый показатель защищенности ОКИИ l -го уровня.

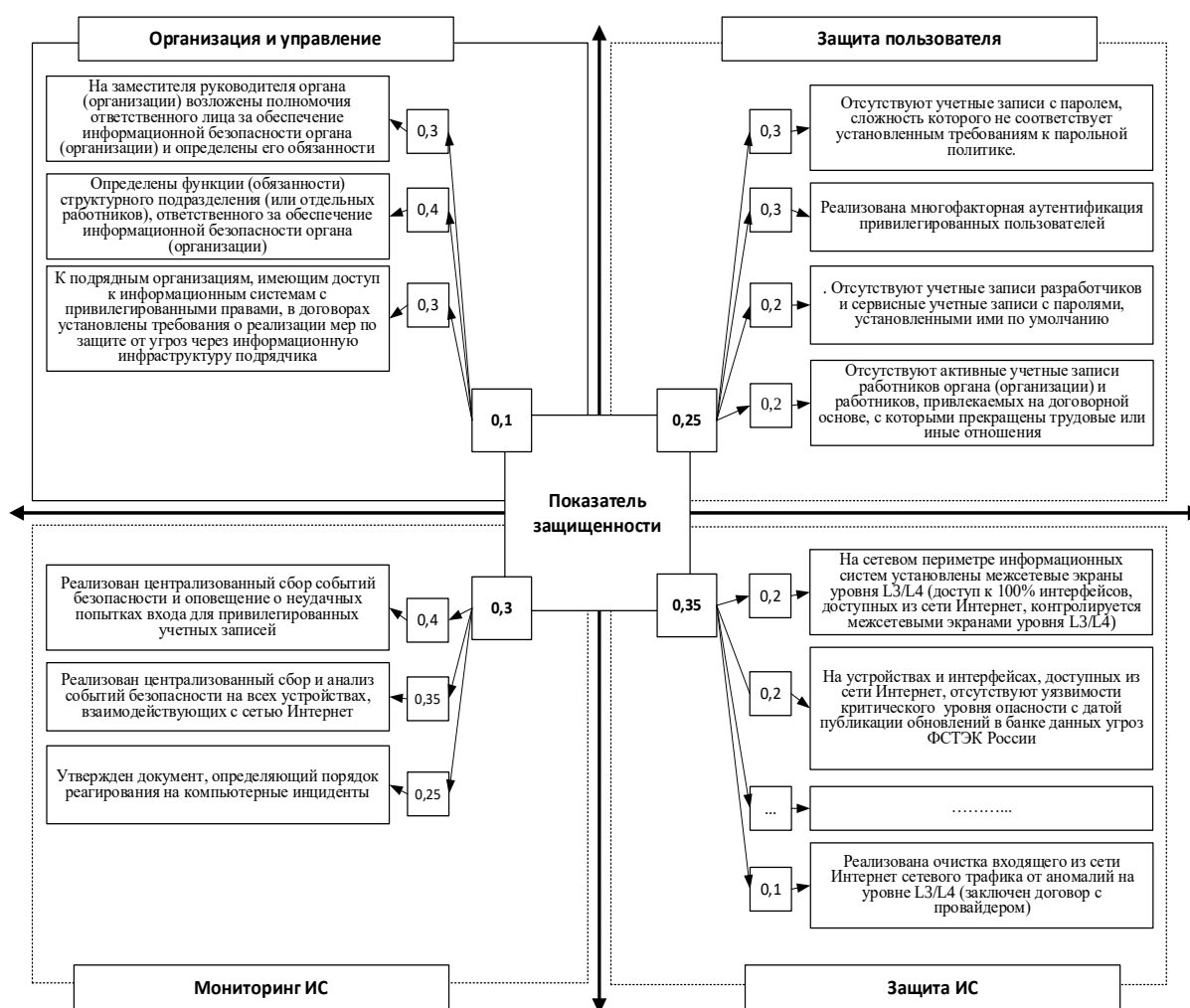


Рис. 1. Декомпозиция интегрального показателя состояния технической защиты

1.3 Определение нормативных и фактических показателей защищенности. Для каждого показателя из (1) задаются нормированные значения соответствия, взятые из нормативно-правовой базы – $x_i^{l, norm} m(0,1]$ и фактические нормированные значения показателей на момент времени t – $x_i^l(t) m(0,1]$. Тогда отклонение фактического значения показателя от нормативного определяется как:

$$x_i^l(t) = |x_i^l(t) - x_i^{l,norm}|. \quad (2)$$

1.4 Для множества (1) осуществляется разбивка и установление укрупненной группы показателей защищенности для l -го уровня ОКИИ, в зависимости от цели назначения:

$$X^l = \bigcup_{j=1}^M X_j^l, \quad X_j^l \cap X_k^l = \emptyset, \quad j \neq k, \quad (3)$$

где $X_j^l \in X^l$ – множество показателей, формирующих j -ю укрупненную группу l -го уровня.

Шаг 2. Введение весовых коэффициентов значимости:

2.1 Для каждой группы укрупненных показателей X_j^l осуществляется получение оценки значимости a_j , $j = \overline{1, M}$, с условием нормировки $\sum_{j=1}^M a_j = 1$, $0 \leq a_j \leq 1$, где a_j – отражает влияние j -й группы на интегральный показатель защищенности ОКИИ.

2.2 Для каждого частного показателя внутри группы осуществляется получение оценки значимости $\omega_{i|j}^l$, с условием нормировки $\sum_{x_i^l \in X_j^l} \omega_{i|j}^l = 1$, $0 \leq \omega_{i|j}^l \leq 1$, где $\omega_{i|j}^l$ – отражает вклад i -го показателя в укрупненный показатель группы j .

Шаг 3. Вычисление нормативного интегрального показателя защищенности на основе аддитивной свертки для укрупненной группы показателей как:

$$X_j^{l,norm} = \sum_{x_i^l \in X_j^l} \omega_{i|j}^l x_i^{l,norm}, \quad (4)$$

и фактического показателя для укрупненной группы показателей:

$$X_j^l(t) = \sum_{x_i^l \in X_j^l} \omega_{i|j}^l x_i^l(t). \quad (5)$$

Для нормативного интегрального показателя защищенности ОКИИ:

$$X^{norm} = \sum_{j=1}^{M_l} a_j X_j^{l,norm}, \quad (6)$$

и фактического интегрального показателя защищенности ОКИИ

$$X(t) = \sum_{j=1}^{M_l} a_j X_j^l(t). \quad (7)$$

Шаг 4. Мониторинг показателей защищенности за заданный период времени с фиксацией полученных отклонений (2) и отклонения интегрального показателя от нормативного значения:

$$\Delta X(t) = |X(t) - X^{norm}|. \quad (8)$$

Шаг 5. Введение функция оценки состояния защищенности ОКИИ:

$$S(t) = \varphi(\Delta X(t)), \quad (9)$$

где $S(t)$ – фактическое состояние защищенности ОКИИ в момент времени t , которое задается из множества $S = \{S_1, S_2, \dots, S_D\}$, согласно правилу соотнесения состояния:

$$S(t) = \begin{cases} S_1, \Delta X(t) \leq \delta_1 \\ S_2, \delta_1 < \Delta X(t) \leq \delta_2 \\ \dots\dots\dots \\ S_D, \Delta X(t) > \delta_{D-1} \end{cases}, \quad (10)$$

где δ_k – пороговые значения отклонений.

Шаг 6. По результатам анализа отклонений (2) и оценки состояния защищенности (10) осуществляется формирование выводов о необходимости реализации мероприятия по

обеспечению безопасности ОКИИ. В случае если значение показателей защищенности СЗИ не соответствует показателям, определенным нормативно-правовой базой, то разрабатывается план мероприятий по обеспечению безопасности ОКИИ, с достижением заданного уровня обеспечения безопасности ОКИИ.

Шаг 7. Внеочередная оценка показателя защищенности ОКИИ проводится в органе (организации) в случаях: возникновения значимого события ИБ; изменения архитектуры ИС, АСУ, ИТКС; запроса контролирующего органа.

Предложенный метод оценки защищенности ОКИИ позволяет обеспечить оценку ИБ при динамическом изменении показателей, что формирует целостную картину о его состоянии и дает возможность своевременно выявлять потенциальные угрозы ИБ и отклонения от штатного режима функционирования. Разработанный метод может лечь в основу систем мониторинга и поддержки принятия управленческих решений, позволяя оценивать критичность возникающих нарушений, прогнозировать возможные сценарии развития нарушения ИБ и разрабатывать меры по предотвращению рисков.

Практический пример оценки защищенности

Практическая реализация оценки защищенности выполнена для информационных потоков, циркулирующих в ИС предприятия машиностроительного комплекса, который представляет собой ОКИИ. За основу построения интегрального показателя защищенности был взят показатель состояния технической защиты информации [2], согласно которому интегральная оценка формируется на основании анализа поведения 4-х групп укрупненных показателей: организация и управление; защита пользователей; защита информационных систем; мониторинг информационной безопасности и реагирование, рис. 1. В пределах заданных нормативно-правовой базой коэффициентов значимости сформированы внутригрупповые показатели ИБ. Поскольку одним из основных требований к системе показателей ИБ является возможность их измерения и оценка изменений, то, представленное множество, рис. 1, целесообразно подвергнуть дальнейшей декомпозиции частных показателей третьего уровня, пример которой представлен на рис. 2, на котором для группы «Защита пользователя», показатели выделены в соответствии с [3]. Аналогично в соответствии с нормативно правовой базой выполнена декомпозиция и для других групп показателей. Такой подход позволил сформировать 16 подгрупп показателей нижестоящего уровня, состоящего их 160 показателей, позволяющих осуществлять мониторинг ИБ ОКИИ.

Наименование показателя безопасности	Нормативный показатель	Текущий показатель
Политика идентификации и аутентификации		
Отсутствие учетных записей с паролем, сложность которого не соответствует установленным требованиям к парольной политике.		
Сформирована политика идентификации и аутентификации на основании ГОСТ Р 58833—2020, Выполнение базового набора мер, определенных 17-ым и 21-ым приказами ФСТЭК России	0,05	0,05
ИАФ.0 Регламентация правил и процедур идентификации и аутентификации.	0,05	0,05
ИАФ.1 Идентификация и аутентификация пользователей и иницируемых ими процессов. Реализована многофакторная аутентификация привилегированных пользователей	0,05	0,05
ИАФ.2 Идентификация и аутентификация устройств	0,05	0,05
ИАФ.3 Управление идентификаторами	0,05	0,05
ИАФ.4 Управление средствами аутентификации. Отсутствуют учетные записи с паролем, сложность которого не соответствует установленным требованиям к парольной политике.	0,05	0,05
Всего оцениваемых характеристик	6,00	6,00
Определение значения частного показателя	0,30	0,30

Рис. 2. Построение показателя защита пользователя

Предложенный подход позволяет сформировать многоуровневую систему показателей, учитывающую требования нормативно-правовой базы. Мониторинг динамики изменений значения показателей в иерархической системе, дает возможность зафиксировать фактическое состояние защищенности ОКИИ и отразить нарушения ИБ как на конкретном показателе, так и получить изменения интегральной оценки защищенности ИС ОКИИ в целом. Например, при нарушении безопасности обработки данных, по полученным значениям отклонений от пороговых значений происходит фиксация события нарушения ИБ с автоматическим перерасчетом значений в группе показателей защиты информационных систем, рис. 3, а также с изменением оценки интегрального показателя состояния технической защиты информации, который меняет значение с 1 до 0,96, что отражено оранжевым цветом на рис. 4.

Значение КЗИ	Минимальный уровень защиты от актуальных угроз безопасности информации не обеспечивается, имеются предпосылки реализации актуальных угроз безопасности информации. Уровень состояния защищенности характеризуется как низкий («оранжевый»)				
0,96					
Номер группы показателей	Наименование групп показателей	Номер [i] и наименование показателя безопасности	Нормативное значение частного показателя	Текущее значение частного показателя	Нормативное значение весового коэффициента группы показателей
3.	Защита информационных систем	1. На сетевом периметре информационных систем установлены межсетевые экраны уровня L3/L4 (доступ к 100% интерфейсов, доступных из сети Интернет, контролируется межсетевыми экранами уровня L3/L4)	0,2	0,15	0,35
		2. На устройствах и интерфейсах, доступных из сети Интернет, отсутствуют уязвимости критического уровня опасности с датой публикации обновлений (компенсирующих мер по устранению) в банке данных угроз ФСТЭК России, на официальных сайтах разработчиков, иных открытых источниках более 30 дней или в отношении таких уязвимостей реализованы компенсирующие меры	0,2	0,2	
		3. На пользовательских устройствах и серверах отсутствуют уязвимости критического уровня с датой публикации обновления (компенсирующих мер по устранению) более 90 дней (не менее 90% устройств и серверов) или в отношении таких уязвимостей реализованы компенсирующие меры	0,1	0,1	
		4. Обеспечен документальный или автоматизированный учет пользовательских устройств, серверов и сетевых устройств (не менее 80% устройств и серверов учтено в документах (ведомостях, паспортах, эксплуатационной документации) или в автоматизированных системах (CMDB))	0,1	0,09	
		5. Обеспечена проверка вложений в электронных письмах электронной почты на наличие вредоносного программного обеспечения (проверяются вложения не менее чем на 80% пользовательских устройств)	0,15	0,15	
		6. Обеспечено централизованное управление средствами антивирусной защиты (не менее чем 80% пользовательских устройств контролируются средствами антивирусной защиты с централизованным управлением). При этом обеспечены контроль и установка обновлений баз данных признаков вредоносного программного обеспечения не реже чем 1 раз в месяц	0,15	0,12	
		7. Реализована очистка входящего из сети Интернет сетевого трафика от аномалий на уровне L3/L4 (заключен договор с провайдером)	0,1	0,08	
4.	Мониторинг информационной безопасности и реагирование	1. Реализован централизованный сбор событий безопасности и оповещение о неудачных попытках входа для привилегированных учетных записей	0,4	0,4	0,3
		2. Реализован централизованный сбор и анализ событий безопасности на всех устройствах, взаимодействующих с сетью Интернет	0,35	0,35	
		3. Утвержден документ, определяющий порядок реагирования на компьютерные инциденты	0,25	0,25	

Рис. 3. Пример нарушений показателя состояния технической защиты информации

Применение подобного подхода позволяет не только получить количественные оценки нарушения ИБ, но и визуализировать их. Одним из наиболее удобных для восприятия является построение гистограмм, рис. 4, отражающее динамику изменения группы показателей.

Разработанный метод количественной оценки защищенности информации с группировкой по показателям позволяет учитывать комбинированные нарушения ИБ, возникающие при одновременном или последовательном воздействии нескольких угроз различной направленности на структурно-функциональные элементы ОКИИ, которые при раздельном анализе угроз могут быть не учтены.

Оценка временного промежутка нарушения при заданных стоимостных потерях позволяет перейти от выявления нарушений ИБ к оценке совокупного ущерба, что повышает эффективность мониторинга и управление ОКИИ.

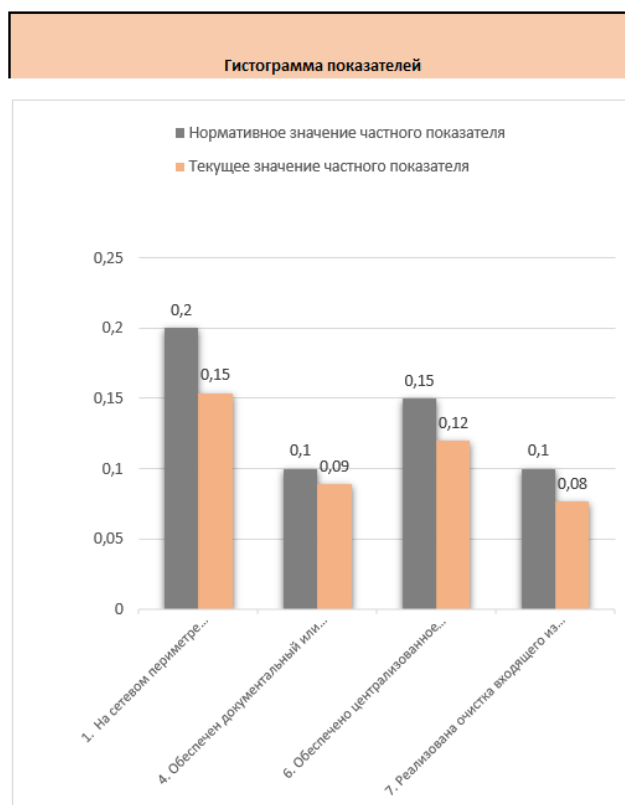


Рис. 4. Гистограмма показателей при возникновении угрозы модификации компонентов

Выводы

Сформированный в результате исследования методический подход отвечает требованиям управления информационной безопасности и способствует повышению устойчивости критически важных объектов за счет прозрачности и воспроизводимости результатов оценки, что создает предпосылки для автоматизации мониторинга и оценки состояния защищенности при динамически изменяющихся угрозах.

Литература

1. Бакшеев А. С., Лившиц И. И. Разработка методики контроля уровня защищенности информации объектов критической информационной инфраструктуры // Вопросы кибербезопасности. 2023. № 2 (54). С. 85-98. DOI 10.21681/2311-3456-2023-2-85-98.
2. Методика оценки показателя состояния технической защиты информации в информационных системах и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Методический документ от 11 ноября 2025 г. – URL: <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-11-noyabrya-2025-g>. (дата обращения: 04.02.2026).
3. Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31. Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. – URL: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31>. (дата обращения: 04.02.2026).
4. Вульфин А. М. Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных // Системная инженерия и информационные технологии. 2023. Т. 5, № 4 (13). С. 50-76. DOI 10.54708/2658-5014-SIT-2023-no3-p50.

5. Журавлева М. Г., Сурова Н. Ю., Хасанова З. Р. Моделирование обеспечения защищенности объектов критической информационной инфраструктуры финансового сектора на основе данных об организационной структуре и управлении // Моделирование, оптимизация и информационные технологии. 2025. Т. 13, № 4 (51). С. 1-15. DOI: 10.26102/2310-6018/2025.51.4.008.
6. Рытов М. Ю., Мусиенко Н. О., Губсков Ю. А., Минин Ю. В. Аудит и мониторинг состояния объектов информатизации в процессе проектирования комплексных систем защиты информации значимых объектов критической информационной инфраструктуры // Приборы и системы. Управление, контроль, диагностика. 2022. № 10. С. 10-18. DOI: 10.25791/pribor.10.2022.1364.
7. Мирошников В. И., Билятдинов К. З., Фортинский А. Г. Повышение качества управленческих решений // Техника средств связи. 2018. № 1 (141). С. 186-189.
8. Фаткиева Р. Р. Система показателей информационной безопасности промышленных предприятий // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2019. № 8. С. 18-27.
9. Двилянсий А. А. Применение методологии тензорного и кластерного анализа для моделирования процессов функционального состояния объектов критической информационной инфраструктуры в условиях деструктивных электромагнитных воздействий // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2025. Т. 15, № 4. С. 175-191. DOI: 10.21869/2223-1536-2025-15-4-175-191.
10. Фисун В. В. Методика оценки защищенности в интеллектуальной системе управления информационной безопасностью объектов критической информационной инфраструктуры // Национальная Ассоциация Ученых. 2022. № 77. С. 59-62. DOI: 10.31618/nas.2413-5291.2022.1.77.575.

References

1. Baksheev A. S., Livshits I. I. *Razrabotka metodiki kontrolya urovnya zashchishchennosti informatsii obektov kriticheskoi informatsionnoi infrastrukturi* [Development of a methodology for monitoring the information security level of critical information infrastructure facilities]. *Cybersecurity issues*, 2023, no 2(54), pp. 85-98. DOI: 10.21681/2311-3456-2023-2-85-98 (in Russian).
2. Methodology for assessing the indicator of the state of technical protection of information in information systems and ensuring the security of significant objects of the critical information infrastructure of the Russian Federation. Methodological document dated November 11, 2025. Available at: <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-11-noyabrya-2025-g> (accessed 04 January 2026) (in Russian).
3. Federal Service for Technical and Export Control. Order no. 31 dated March 14, 2014. On approval of requirements for information security in automated control systems for production and technological processes at critical facilities, potentially dangerous facilities, as well as facilities that pose an increased danger to human life and health and to the environment. Available at: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31> (accessed 04 January 2026) (in Russian).
4. Vulfin A. M. *Modeli i metodi kompleksnoi otsenki riskov bezopasnosti obektov kriticheskoi informatsionnoi infrastrukturi na osnove intellektualnogo analiza dannikh* [Models and methods of integrated assessment of security risks of critical information infrastructure facilities based on data mining]. *System engineering and information technology*, 2023, v. 5, no. 4 (13), pp. 50-76 (in Russian). DOI: 10.54708/2658-5014-SIIT-2023-no3-p50.
5. Zhuravleva M. G., Surova N. Yu., Khasanova Z. R. *Modelirovanie obespecheniya zashchishchennosti obektov kriticheskoi informatsionnoi infrastrukturi finansovogo sektora na osnove dannikh ob organizatsionnoi strukture i upravlenii* [Modeling the security of critical information infrastructure facilities in the financial sector based on organizational structure and management data]. *Modeling, optimization, and information technology*, 2025, v. 13, no. 4 (51), pp. 1-15 (in Russian). DOI: 10.26102/2310-6018/2025.51.4.008.
6. Rytov M. Yu., Musienko N. O., Gubskov Yu. A., Minin Yu. V. *Audit i monitoring sostoyaniya obektov informatizatsii v protsesse proektirovaniya kompleksnykh sistem zashchiti informatsii znachimikh obektov kriticheskoi informatsionnoi infrastrukturi* [Audit and monitoring of the state of informatization facilities in the process of designing integrated information security systems for significant critical

information infrastructure facilities]. *Devices and Systems. Management, monitoring, diagnostics*, 2022, no. 10, pp. 10-18 (in Russian). DOI: 10.25791/pribor.10.2022.1364.

7. Miroshnikov V. I., Bilyatdinov K. Z., Fortinsky A. G. *Povishenie kachestva upravlencheskikh reshenii* [Improving the quality of management decisions] *Communications equipment*, 2018, no. 1 (141), pp. 186-189 (in Russian).

8. Fatkueva R. R. *Sistema pokazatelei informatsionnoi bezopasnosti promishlennikh predpriyatii* [System of information security indicators for industrial enterprises]. *Scientific and technical information. Ser. 2: Information processes and systems*, 2019, no. 8, pp. 18-27 (in Russian).

9. Dviliansky A. A. *Primenenie metodologii tenzornogo i klasternogo analiza dlya modelirovaniya protsessov funktsionalnogo sostoyaniya obektov kriticheskoi informatsionnoi infrastrukturi v usloviyakh destruktivnykh elektromagnitnykh vozddeystvii* [Application of tensor and cluster analysis methodology for modeling the processes of the functional state of critical information infrastructure facilities under destructive electromagnetic influences] *Proceedings of the Southwestern State University. Series: Management, computer engineering, computer science. Medical instrumentation*, 2025, v. 15, no. 4, pp. 175-191 (in Russian). DOI: 10.21869/2223-1536-2025-15-4-175-191

10. Fisun V. V. *Metodika otsenki zashchishchennosti v intellektualnoi sisteme upravleniya informatsionnoi bezopasnostyu obektov kriticheskoi informatsionnoi infrastrukturi* [Methodology for assessing security in an intelligent information security management system for critical information infrastructure facilities]. *National Association of Scientists*, 2022, no. 77, pp. 59-62 (in Russian). DOI: 10.31618/nas.2413-5291.2022.1.77.575.

Статья поступила 10 февраля 2026 г.

Информация об авторах

Билятдинов Камиль Закирович – доктор технических наук, кандидат военных наук, доцент. Профессор кафедры 25. Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения». Область научных интересов: связь, автоматизация, информационная безопасность, управление. Тел.: +7(812)310-34-72. E-mail: inib@pgups.ru.

Адрес: 190000, Россия, Санкт-Петербург, Б. Морская ул., 67.

Фаткуева Роза Равильевна – кандидат технических наук, доцент. Доцент кафедры. Федеральное государственное бюджетное образовательное учреждение высшего образования «Петербургский государственный университет путей сообщения Императора Александра I». Область научных интересов: мониторинг информационной безопасности; безопасность сетевого трафика; моделирование информационных систем; сбор и обработка информации. E-mail: rikki2@yandex.ru.

Адрес: 190031, Россия, Санкт-Петербург, Московский пр., д. 9.

Фортинский Андрей Григорьевич – кандидат технических наук. Заместитель генерального директора по научной работе. Акционерное общество «Научно-исследовательский институт «Масштаб». Область научных интересов: моделирование информационных систем, системный анализ, теория управления. E-mail: info@mashtab.org.

Адрес: 194100, Россия, Санкт-Петербург, ул. Кантемировская, д. 5.

Method for assessing the information security of a critical information infrastructure facility

R. R. Fatkueva, K. Z. Bilyatdinov, A. G. Fortinsky

Annotation. Problem statement: *The functioning of critical information infrastructure facilities in modern conditions is characterized by an increase in the number of threats. In this regard, there is an increasing need to assess the level of information security in them. There is a problem of transition from periodic to continuous monitoring of the security status of information processing and transmission.*

However, at present, models and methods that allow for formalized consideration of the dynamics of changes in information security indicators remain insufficiently developed, which limits the possibility of timely detection of security breaches. **Purpose:** the aim is to develop a scientific and methodological framework for the integrated assessment of information security based on a set of specific indicators, taking into account their significance. **Methods:** the research employed methods of systems analysis, multi-criteria evaluation of protection levels, vulnerability and threat assessment, as well as scenario modelling of potential security incidents. **Results:** a method for quantifying information security and information security of a critical information infrastructure facility has been developed. **Novelty:** the problem is that the proposed integrated assessment of information security takes into account the dynamics of changes in particular indicators over time and formalizes quantitative indicators based on their significance. Dividing the indicators into groups allows you to expand its composition, if necessary. This provides a more accurate reflection of the real state of information security of the analyzed object and allows timely detection of destructive effects. **Practical relevance:** the proposed approach can be used to support management decisions, plan information security measures, and compare the security level of various critical infrastructure facilities. The results obtained can later be used to quantify and monitor other parameters of complex technical systems.

Keywords: the object of critical information infrastructure, information security, information security index, integrated assessment, private indicators, multi-criteria assessment, information security risk assessment.

Information about the authors

Kamil Zakirovich Bilyatdinov – Doctor of Technical Sciences, Candidate of Military Sciences, Associate Professor. Professor of Department 25 of the Federal State Autonomous Educational Institution of Higher Education «Saint Petersburg State University of Aerospace Instrumentation». Research interests: communications, automation, information security, management. Tel.: +7(812)310 34 72. E-mail: inib@pgups.ru.

Address: 190000, Russia, Saint-Petersburg, Bolshaya Morskaya St., 67.

Roza Ravilyevna Fatkueva – Candidate of Technical Sciences, Associate Professor. Associate Professor of the Department of Informatics and Information Security at the Emperor Alexander I St. Petersburg State Transport University. Research interests: information security monitoring; network traffic security; information system modeling; information collection and processing. E-mail: rikki2@yandex.ru.

Address: 190031, Russia, Saint Petersburg, Moskovsky ave. 9.

Andrey Grigorievich Fortinsky – Candidate of Technical Sciences. Deputy General Director for Scientific Work at JSC Scientific Research Institute «Mashtab». Research interests: modeling of information systems, system analysis, management theory. E-mail: info@mashtab.org.

Address: 194100, Russia, Saint Petersburg, Kantemirovskaya str., 5.

Для цитирования:

Фаткуева Р. Р., Билиятдинов К. З., Фортинский А. Г. Метод оценки защищенности информации и информационной безопасности объекта критической информационной инфраструктуры // Техника средств связи. 2026. № 2 (174). С. 21-30. DOI: 10.24412/2782-2141-2026-2-21-30.

For citation:

Fatkueva R. R., Bilyatdinov K. Z., Fortinsky A. G. Method for assessing the information security of a critical information infrastructure facility. *Means of Communication Equipment*, 2026, no. 2 (174), pp. 21-30 (in Russian). DOI: 10.24412/2782-2141-2026-2-21-30.

Метод управления информационной безопасностью и восстановления информационных систем на основе реконфигурации объекта критической инфраструктуры

Фаткиева Р. Р., Билятдинов К. З., Фортинский А. Г.

Аннотация. *Постановка задачи* существующие подходы к обеспечению информационной безопасности и восстановлению объектов критической инфраструктуры ориентированы на регламентные меры защиты, локальное реагирование на угрозы и реализуются без учета взаимосвязи между требованиями безопасности, доступности и временем восстановления. В связи с этим возникает необходимость в разработке методологического аппарата, позволяющего учитывать взаимозависимость критериев безопасности и ресурсных ограничений при восстановлении. **Целью работы** является разработка методов управления информационной безопасностью и восстановлением систем, обеспечивающих целенаправленную реконфигурацию их структуры. **Используемые методы:** исследование выполнено с применением методов системного анализа, многокритериальной оценки показателей, анализа уязвимостей и угроз, аппарата иерархической многокритериальной оптимизации. **Результат:** предложен метод управления, основанный на представлении процесса достижения требуемого состояния в виде дерева решений, что позволяет учитывать альтернативные маршруты реконфигурации по заданной целевой функции. **Новизна:** заключается в переносе аппарата целевой функции реконфигурации в область управления информационной безопасностью. **Практическая значимость:** заключается в возможности моделирования альтернативных вариантов управления и выбора оптимального решения, обеспечивающего установление заданного уровня информационной безопасности и функциональной готовности объектов критической инфраструктуры.

Ключевые слова: восстановление систем, информационная безопасность, объект критической информационной инфраструктуры, оптимизационные модели, принятие решений, управление информационной безопасностью, устойчивость и живучесть, функция полезности.

Актуальность

В современных условиях успешность управления объектом критической информационной инфраструктуры (ОКИИ) зависит от скорости реакции на то или иное изменение его поведения, применяемых принципов и методов управления, способов их синтеза, а также воздействия окружающей среды. Подходы к управлению определяются характером используемой в ОКИИ информации и степенью обеспечения информационной безопасности (ИБ). К основным этапам управления можно отнести: анализ текущего состояния, оценка показателей функционирования; условия достижения стратегических целей; формирование управляющих воздействий. В случае несоответствия эффективности управляющих воздействий или влиянии информационных угроз возникает необходимость разработки оптимальных методов реконфигурации и восстановления ОКИИ. Однако условия динамически развивающегося пространства угроз требует учета значительного числа параметров реконфигурируемой системы. В этой ситуации обеспечение высокой доступности и непрерывности работы критических процессов может вступать в противоречие с задачей усиления безопасности, поскольку в процессе перенастройки параметров безопасности или изменения архитектуры ОКИИ возникают временные окна уязвимостей (рис. 1). При этом реконфигурация архитектуры ОКИИ требует тщательного тестирования на обеспечение гибкости, устойчивости и совместимости как для введенных средств, так и для уже задействованных ресурсов, что сказывается на скорости внедрения изменений и влечет за собой запаздывание в обеспечении должного уровня ИБ [2-7].

С другой стороны, необходимость реконфигурации ОКИИ может вызвать проблемы с совместимостью старых и новых технологий или применяемого программного обеспечения, что ведет к нарушению обработки информации, поскольку влечет за собой риск стабильности работы ОКИИ. В то же время, слишком длительные и осторожные изменения приводят к затягиванию процесса, снижая безопасность в условиях быстроменяющихся деструктивных воздействий [8].

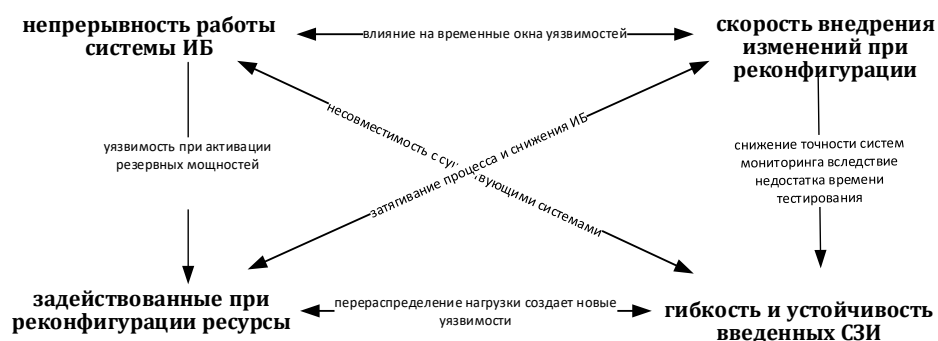


Рис. 1. Взаимосвязь требований системы реконфигурации

В этих условиях существующие в настоящее время методы восстановления, реконфигурации и живучести ориентированы либо на доступность, либо на безопасность, но не на одновременное изменение этих параметров [9, 10]. Практически отсутствуют формализованные методы, которые переводили бы требования безопасности и восстановления в математические или алгоритмические модели [11].

Таким образом, совершенствование методологического аппарата управления информационной безопасностью и восстановлением информационных систем ОКИИ является актуальной научно-практической задачей, направленной на повышение устойчивости ОКИИ в условиях современных угроз.

Метод управления информационной безопасностью и восстановления информационных систем на основе реконфигурации объекта критической инфраструктуры

Исследование основных характеристик процесса перестроения структуры ОКИИ показал, что формирование процесса реконфигурации ОКИИ направлено на соблюдение баланса между безопасностью, гибкостью и экономической эффективностью, временем внедрения изменений, затрат на ресурсы, а также необходимостью учета стоимости реконфигурации и потенциальных потерь в случае угрозы нарушения ИБ (рис. 1). Возникает необходимость учета всех вышеперечисленных требований при построении системотехнического решения, позволяющего обеспечить реконфигурацию ОКИИ. Рассмотрим их более подробно. В ходе анализа требований установлено, что в зависимости от применяемой архитектуры ОКИИ их возможно классифицировать по типу оптимизационной функции от минимизации до максимизации вклада в целевую функцию ОКИИ (табл. 1).

Анализ и учет выдвинутых требований дает возможность перейти к построению целевой функции реконфигурации ОКИИ. Однако здесь появляются трудности в поиске нового состава ОКИИ, поскольку возникает необходимость учета большего количества переменных, имеющих вложенную структуру. Для преодоления этого целесообразно воспользоваться аппаратом иерархического многокритериального анализа и оптимизации, с использованием дерева целевой функции, в виде ориентированного ациклического графа с иерархической структурой, где узлы – уровни декомпозиции целевой функции, согласно переменным, представленным в табл. 1.

Определим метод в виде последовательности шагов, позволяющих осуществить формирование дерева и целевой функции как:

1. Выделение ключевой проблемы, решение которой требует применения аппарата реконфигурации ОКИИ.
2. Построение требований (показателей) к реконфигурируемой структуре ОКИИ и/или процессу реконфигурации путем формирования оптимизационных задач, необходимых для построения целевой функции реконфигурации.
3. Декомпозиция и уточнение требований в виде формирования множества переменных, удовлетворяющих новую структуру ОКИИ (и/или процесс реконфигурации). В случае отсутствия вложенной структуры шаг можно пропустить.

4. Построение маршрута достижения целевой функции реконфигурации в виде дерева, с учетом требований выдвинутых на шаге 2.
5. Поиск маршрута достижения целевой функции на дереве и формирование целевой функции удовлетворяющих требованиям, полученным на шаге 3.
6. Моделирование альтернативных вариантов реконфигурации ОКИИ, их сравнительный анализ и выбор оптимального решения с учетом введенных ограничений.

Таблица 1 – Взаимосвязь функций и требований процесса реконфигурации

Требование	Функция минимизации	Функция максимизации
Непрерывность работы системы	$R_{HP}^{\min} = \min \left(\sum_{i=1}^N T_R \right) / T,$ где T_R – допустимые временные перебои p -го ресурса при внедрении изменений; T – общее время процесса обработки информации	$R_{HP}^{\max} = \max T,$ где T – общее время работы процесса обработки информации в условиях внедрения изменений
Скорость внедрения изменений	$R_{COI}^{\max} = \sum_{j=1}^M N_j(COI) / \min T,$ где $N_j(COI)$ – количество успешно внедренных изменений от j -ой угрозы; T – время, затрачиваемое на внедрение	
Задействованные при реконфигурации ресурсы	$R_{KII}^{\min} = \min \left(\left(\sum_{l=1}^K R_l \right) / R, \sum_{i=1}^N (T_i \cdot x_i) \right),$ где R_l – задействованные ресурсы; R – общее количество ресурсов	$R_{KII}^{\max} = \max \left(\left(\sum_{l=1}^K R_l \right) / R, \min \sum_{i=1}^N (T_i \cdot x_i) \right),$ где R_l – задействованные ресурсы; R – общее количество ресурсов
Гибкость введенных средств защиты информации (СЗИ)	$R_{IC}^{\min} = \min \sum_{i=1}^N S_{CЗИам} / S_{CЗИ},$ где $S_{CЗИам}$ – СЗИ, требующие замены; $S_{CЗИ}$ – общее количество СЗИ	$R_{IC}^{\max} = \max \sum_{i=1}^N S_{CЗИадап} / S_{CЗИ},$ где $S_{CЗИадап}$ – адаптированные к новым угрозам СЗИ; $S_{CЗИ}$ – общее число СЗИ
Устойчивость внедренных СЗИ (УСЗИ)	Интегральный показатель устойчивости ОКИИ может быть представлен в виде: $R_{YCЗИ} = \omega_1 \cdot R_{YCЗИ}(D) + \omega_2 \cdot R_{YCЗИ}(Y) + \omega_3 \cdot R_{YCЗИ}(H),$ где $R_{YCЗИ}(D)$ – доступность; $R_{YCЗИ}(Y)$ – устойчивость к атакам; $R_{YCЗИ}(H)$ – устойчивость к отказам; $\omega_1 - \omega_3$ – весовые коэффициенты. Тогда задачу минимизации можно выразить как: $R_{YCЗИ}(D) = R_{HP}^{\min}, R_{YCЗИ}(Y) = \min P_j(Y_j), R_{YCЗИ}(H) = e^{\min(-\lambda)t},$ где $P_j(Y_j)$ – вероятность совершения угрозы; λ – интенсивность отказов; t – среднее время наработки на отказ.	
Риск возникновения уязвимостей после реконфигурации	$R_Y^{\min} = \min \sum_{j=1}^N Y_j(t),$ где Y_j – показатель новых уязвимостей, возникающих при изменениях	$R_Y^{\max} = \max \sum_{j=1}^N Y'_j(t),$ где $Y'_j(t)$ – показатель учтенных рисков при реконфигурации

При необходимости данные шаги могут выполняться итеративно, с возвратом к предыдущим этапам для уточнения проблемы, требований и структуры решения до получения приемлемого и обоснованного решения задачи реконфигурации ОКИИ.

Реконфигурация информационной системы при воздействии угроз

Проанализируем подходы к управлению ИБ и восстановлению информационной системы (ИС) на примере формализации целевой функции реконфигурации ОКИИ. В качестве сценария нарушения ИБ проведем моделирование угрозы модификации (искажения) информационных элементов, вызванное эксплуатацией уязвимостей

программного обеспечения. Ключевая проблема на шаге 1 выделена как невозможность гарантии целостности данных и корректности функционирования системы в условиях эксплуатируемой уязвимости программного обеспечения при сохранении требуемого уровня доступности сервисов, что влечет за собой необходимость реконфигурации ОКИИ. Согласно шагу 2 осуществим построение требований к процессу реконфигурации, в частности: стоимость вносимых при реконфигурации изменений не должна превышать допустимые потери от временных перебоев, при этом непрерывность работы ОКИИ после реконфигурации должна быть выше, чем до внесения изменений. Ресурсы, задействованные в процессе реконфигурации должны быть минимизированы, поскольку если изменения требуют слишком много ресурсов, то это может отрицательно сказаться на доступности ОКИИ, таким образом сформированные ограничения гарантирует, что реконфигурация не приведет к деградации процессов ОКИИ. Необходимо предусмотреть что если внедрение новых средств защиты информации приводит к чрезмерным компромиссам (например, сильному усложнению архитектуры, снижению скорости обработки данных), то их эффективность может также оказаться ниже, чем сами потери от угроз. Введенные ограничения позволяют сбалансировать безопасность и экономическую целесообразность.

На шаге 3 осуществим формализацию требований в виде формирования множества переменных, взятых из табл. 1. Для построений целевой функции обработки информации W^N , согласно шага 2 определим множество переменных, входящих в ее состав: $R^{\max}_{HP}$, $R^{\min}_{HP}$, $R^{\max}_{COI}$, $R^{\min}_{КП}$, $R^{\min}_{ГС}$, $R^{\min}_Y$, $R^{\max}_{ГС}$, $R^{\max}_Y$, $R^{\max}_{КП}$. Это позволяет перейти к построению маршрута достижения целевой функции реконфигурации в виде дерева (рис. 2).

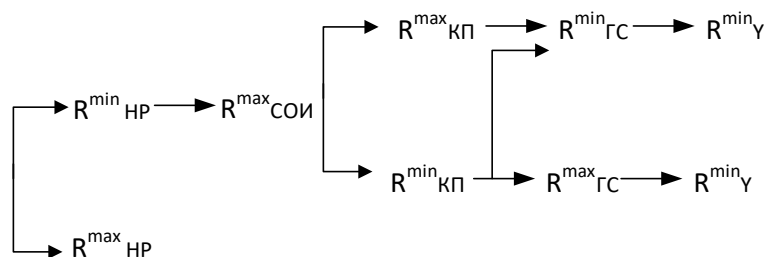


Рис. 2. Построение дерева целевой функции процесса реконфигурации

Проанализируем дерево, представленное на рис. 2, рассмотрим возможные маршруты и построим возможные целевые функции реконфигурации W^N :

$$W^N \rightarrow R^{\min}_{HP} (R^{\max}_{COI} (R^{\min}_{КП}, R^{\min}_{ГС} (R^{\min}_Y))), \quad (1)$$

$$W^N \rightarrow R^{\min}_{HP} (R^{\max}_{COI} (R^{\min}_{КП}, R^{\max}_{ГС} (R^{\min}_Y))), \quad (2)$$

$$W^N \rightarrow R^{\min}_{HP} (R^{\max}_{COI} (R^{\max}_{КП}, R^{\min}_{ГС} (R^{\min}_Y))), \quad (3)$$

при условии $T(R^{\max}_{HP}) < T_{обр}$, где $T_{обр}$ – время обработки полного цикла информации.

Нетрудно видеть, что если основное различие между маршрутами заключается в задействованных при реконфигурации ресурсах ($R^{\min}_{КП}$ и $R^{\max}_{КП}$), влияющих на обеспечение ИБ ОКИИ и скорость обработки информации, то структура целевых функций реконфигурации (1) – (3) сводится к оценке функции полезности Кобба-Дугласа: $U_i(\Delta T_{защ}) = A_i \cdot \Delta I_i^{\alpha} \cdot \Delta T_i^{\beta} \cdot \Delta T_{защ i}$, где A_i – технологический коэффициент, отражающий успешность реконфигурации; ΔI – количество обрабатываемой информации; ΔT – время обработки информации; $T_{защ i}$ – время затрачиваемое средствами защиты информации на обеспечение ее безопасности; α и β – коэффициенты эластичности, которые в частном виде $\alpha = 1$ и $\beta = -1$.

Учет динамики переменных в функции полезности (1) позволяет осуществить оценку изменения информационных потоков при реконфигурации ИС ОКИИ и подобрать оптимальные средства защиты информации для исключения угрозы модификации (искажения) информационных элементов, вызванное эксплуатацией уязвимостей программного обеспечения.

Для устранения угрозы было сформировано 3 варианта реконфигурации процесса обработки информации, которые включают: 1 – полный аудит системы информационной безопасности (t_8); 2 – обновление программного обеспечения (t_2); закрытие неиспользуемых портов (t_3); ограничение прав доступа (t_4); 3 – настройка системы мониторинга (t_5), обновление программного обеспечения (t_2), обучение сотрудников (t_6), тестирование (t_7).

Оценка изменения информационного потока показала, что для первого варианта реконфигурации имеется плавное, стабильное снижение информационного потока на все временном интервале реконфигурации, табл. 2. Первый вариант быстро стабилизирует поток за счёт последовательного аудита и формирования мер безопасности.

Таблица 2 – Динамика изменения информационных потоков при реконфигурации

Вариант реконфигурации	Потоки								
	Поток нарушений	Обновление программного обеспечения	Закрытие неиспользуемых портов	Ограничение прав доступа пользователей	Настройка системы мониторинга	Обучение сотрудников безопасности	Проведение регулярных тестов на проникновение	Проведение полного аудита безопасности	Итоговый поток с нарушениями
1	31352	30752	30352	29852	29452	20	29252	29252	0
2	31352	30752	30352	29852	29852	29852	29852	29852	29852
3	31352	30752	30752	30752	30352	30152	29152	29152	29152

Использование второго варианта имеет схожую картину до момента времени t_5 , где информационный поток перестает реагировать на предпринятые изменения (рис. 2), его значения фиксируется, то есть имеет место исчерпание потенциала реконфигурации.

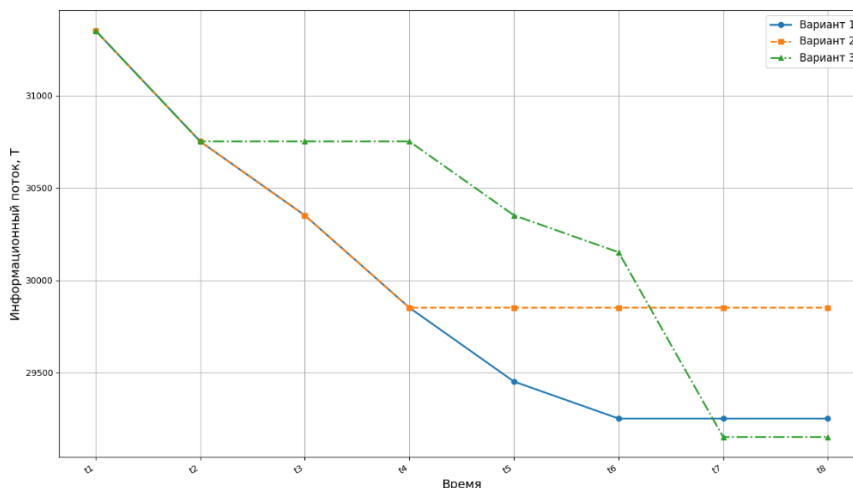


Рис. 2. Временная оценка изменения информационного потока при реконфигурации

Анализ результатов применения третьего варианта реконфигурации в отличие от второго свидетельствует об отложенном эффекте реконфигурации, когда реальные изменения начинают проявляться только на поздних временных интервалах, что может свидетельствовать о высокой зависимости от человеческого фактора (обучение, тесты).

Таким образом моделирование результатов реконфигурации позволяет осуществить оценку успешности введенных мероприятий по обеспечению ИБ, например, в случае если необходима ранняя стабилизация и минимальные потери, то целесообразно использовать первый вариант, если экономия ресурсов – второй вариант, если причиной нарушения является в первую очередь человеческий фактор, то предпочтительнее третий вариант.

Выводы

Представленный метод позволяет перейти к управлению информационной безопасностью ОКИИ за счет декомпозиции требований к структуре и процессам, а также построения маршрутов достижения целевого состояния безопасности. Использование целевой функции обеспечивает согласование требований защищенности, устойчивости и доступности с учетом ограниченности ресурсов и времени восстановления.

К дальнейшим направлениям развития метода целесообразно отнести расширение состава показателей целевой функции и возможности ее интеграции в состав систем поддержки принятия решений, что позволит повысить оперативность и адаптивность восстановления ОКИИ в условиях динамически изменяющихся угроз.

Литература

1. Маслобоев А. В., Цыгичко В. Н. Адаптация и развитие рискориентированной методологии обеспечения безопасности критически важных объектов к управлению жизнеспособностью критических инфраструктур // Надежность и качество сложных систем. 2024. № 4. С. 140–159. DOI: 10.21685/2307-4205-2024-4-16.
2. Краснов А. Е., Мосолов А. С., Феоктистова Н. А. Оценивание устойчивости критических информационных инфраструктур к угрозам информационной безопасности // Безопасность информационных технологий. 2021. Т. 28, № 1. С. 106–120. DOI: 10.26583/bit.2021.1.09.
3. Гавдан Г. П., Вавичкин А. Н., Иваненко В. Г. Устойчивость технологических процессов в аспекте безопасности критической информационной инфраструктуры // Безопасность информационных технологий. 2023. Т. 30, № 2. С. 38–52. DOI: 10.26583/bit.2023.2.02.
4. Максимова Е. А., Буйневич М. В. Метод оценки инфраструктурной устойчивости субъектов критической информационной инфраструктуры // Вестник УрФО. Безопасность в информационной сфере. 2022. № 1(43). С. 50–63. DOI: 10.14529/secur220107.
5. Гавдан Г. П., Иваненко В. Г., Рыбалко Э. П., Рыбалко Д. П. Устойчивость функционирования объектов критической информационной инфраструктуры // Безопасность информационных технологий. 2022. Т. 29, № 4. С. 53–66. DOI: 10.26583/bit.2022.4.05.
6. Халиуллина Д. Н., Быстров В. В. Жизнеспособность критических инфраструктур региональной безопасности // Труды Кольского научного центра РАН. Информационные технологии. Вып. 12. 2021. Т. 12, № 5. С. 104–116. <http://dx.doi.org/10.37614/2307-5252.2021.5.12.009>.
7. Дорошенко И. Е., Максудов М. О., Селифанов В. В. Вопросы формирования организационно-функциональной структуры системы управления информационной безопасностью значимого объекта критической информационной инфраструктуры // Интерэкспо Гео-Сибирь. 2022. Т. 6. С. 47–53. DOI: 10.33764/2618-981X-2022-6-47-53.
8. Середа Л. А., Гребенюк Г. Г. Алгоритмы приоритизации при восстановлении поврежденных объектов критических инфраструктур // Computational nanotechnology. 2025. Т. 12. № 5. С. 179–189. DOI: 10.33693/2313-223X-2025-12-5-179-189.
9. Vaudey J., Mocanu S., Rutten E. *et al.* Self-Reconfiguration of Industrial Control Systems as a Response to Cyberattacks. *J Netw Syst Manage* 34, 4 (2026). <https://doi.org/10.1007/s10922-025-09979-0>.
10. Huang S., Mo G., Jing S., Leng J., Li X., Gu X., Yan Y., Wang G. Digital twin-driven self-adaptive reconfiguration planning method of smart manufacturing systems using game theory and deep Q-network for industry 5.0 // *Journal of Industrial Information Integration*, 2025, vol. 47, 100901. <https://doi.org/10.1016/j.jii.2025.100901>.
11. Fang Z., Li H., Chen D. An Integrated Method for Selecting Architecture Alternatives and Reconfiguration Options Towards System-of-Systems Resilience. *Systems* 2025, 13, 9. <https://doi.org/10.3390/systems13010009>.

References

1. Masloboev A.V., Tsygichko V. N. *Adaptaciya i razvitie riskorientirovannoj metodologii obespecheniya bezopasnosti kriticheski vaznyh ob"ektov k upravleniyu zhiznesposobnost'yu kriticheskikh infrastruktur* [Adaptation and development of a risk-based methodology for ensuring the safety of critical

facilities for managing the viability of critical infrastructures]. *Reliability and quality of complex systems*, 2024, no. 4, pp. 140-159 (in Russian). DOI: 10.21685/230742052024416.

2. Krasnov A. E., Mosolov A. S., Feoktistova N. A. *Ocenivanie ustojchivosti kriticheskikh informacionnykh infrastruktur k ugrozam informacionnoj bezopasnosti* [Assessing the resilience of critical information infrastructures to information security threats]. *Information technology security*, 2021, vol. 28, no. 1, pp. 106-120 (in Russian). DOI: 10.26583/bit.2021.1.09.

3. Gavdan G. P., Vavichkin A. N., Ivanenko V. G. *Ustojchivost' tekhnologicheskikh processov v aspekte bezopasnosti kriticheskoy informacionnoj infrastruktury* [Sustainability of technological processes in the aspect of security of critical information infrastructure]. *Information technology security*, 2023, vol. 30, no. 2, pp. 38-52 (in Russian). DOI: 10.26583/bit.2023.2.02.

4. Maksimova E. A., Buinevich M. V. *Metod ocenki infrastrukturnoj ustojchivosti sub"ektov kriticheskoy informacionnoj infrastruktury* [A method for assessing the infrastructural stability of subjects of critical information infrastructure]. *Bulletin of the Ural Federal District. Information security*, 2022, no 1(43), pp. 50-63 (in Russian). DOI: 10.14529/secur220107.

5. Gavdan G. P., Ivanenko V. G., Rybalko E. P., Rybalko D. P. Stability of functioning of critical information infrastructure facilities. *Information technology security*, 2022, vol. 29, no. 4, pp. 53-66 (in Russian). DOI: 10.26583/bit.2022.4.05.

6. Khaliullina D. N., Bystrov V. V. *Zhiznesposobnost' kriticheskikh infrastruktur regional'noj bezopasnosti* [Viability of critical regional security infrastructures]. *Proceedings of the Kola Scientific Center of the Russian Academy of Sciences. Information technology*, 2021, vol. 12, no. 5, pp. 104-116 (in Russian). <http://dx.doi.org/10.37614/2307-5252.2021.5.12.009>.

7. Doroshenko I. E., Maksudov M. O., Selifanov V. V. *Voprosy formirovaniya organizacionno-funkcional'noj struktury sistemy upravleniya informacionnoj bezopasnost'yu znachimogo ob"ekta kriticheskoy informacionnoj infrastruktury* [Issues of formation of the organizational and functional structure of the information security management system of a significant object of critical information infrastructure]. *Interexpo Geo-Siberia*, 2022, vol. 6, pp. 47-53 (in Russian). DOI: 10.33764/2618-981X-2022-6-47-53.

8. Sereda L. A., Grebenyuk G. G. Prioritization algorithms for restoring damaged critical infrastructure facilities. *Computational nanotechnology*, 2025, vol. 12, no. 5, pp. 179-189 (in Russian). DOI: 10.33693/2313-223X-2025-12-5-179-189.

9. Vaudey J., Mocanu S., Rutten E. *et al.* Self-Reconfiguration of Industrial Control Systems as a Response to Cyberattacks. *J Netw Syst Manage* 34, 4 (2026). <https://doi.org/10.1007/s10922-025-09979-0>.

10. Huang S., Mo G., Jing S., Leng J., Li X., Gu X., Yan Y., Wang G. Digital twin-driven self-adaptive reconfiguration planning method of smart manufacturing systems using game theory and deep Q-network for industry 5.0. *Journal of Industrial Information Integration*, 2025, vol.47, 100901. <https://doi.org/10.1016/j.jii.2025.100901>.

11. Fang, Z.; Li, H.; Chen, D. An Integrated Method for Selecting Architecture Alternatives and Reconfiguration Options Towards System-of-Systems Resilience. *Systems*, 2025, 13, 9. <https://doi.org/10.3390/systems13010009>.

Статья поступила 20 февраля 2026 г.

Информация об авторах

Биятдинов Камиль Закирович – доктор технических наук, кандидат военных наук, доцент. Профессор кафедры 25. Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения». Область научных интересов: связь, автоматизация, информационная безопасность, управление. Тел.: +7(812)310 34 72. E-mail: inib@pgups.ru.

Адрес: Россия, 190000, г. Санкт-Петербург, Б. Морская ул., д. 67.

Фаткиева Роза Равильевна – кандидат технических наук, доцент. Доцент кафедры. Федеральное государственное бюджетное образовательное учреждение высшего образования «Петербургский государственный университет путей сообщения Императора Александра I». Область научных интересов: мониторинг информационной безопасности; безопасность сетевого трафика; моделирование информационных систем. E-mail: rikki2@yandex.ru. Адрес: 190031, Россия, Санкт-Петербург, Московский пр., д. 9.

Фортинский Андрей Григорьевич – кандидат технических наук. Заместитель генерального директора по научной работе. АО «НИИ «Масштаб». Область научных интересов: моделирование информационных систем, системный анализ, теория управления. E-mail: info@mashtab.org.

Адрес: Россия, 194100, Санкт-Петербург, ул. Кантемировская, д. 5

Method for managing information security and restoring information systems based on reconfiguration of a critical infrastructure facility

R. R. Fatkueva, K. Z. Bilyatdinov, A. G. Fortinsky

Annotation. Problem statement: existing approaches to ensuring information security and restoring critical infrastructure facilities are focused on routine protection measures, local threat response, and are implemented without taking into account the relationship between security requirements, availability, and recovery time. In this regard, there is a need to develop a methodological framework that allows taking into account the interdependence of safety criteria and resource constraints during recovery. **Purpose:** the aim is to develop methods for managing information security and system recovery that ensure targeted reconfiguration of their structure. **Methods:** the study was performed using methods of system analysis, multi-criteria evaluation of indicators, vulnerability and threat analysis, and hierarchical multi-criteria optimization. **Results:** a control method is proposed based on the representation of the process of achieving the desired state in the form of a decision tree, which allows taking into account alternative reconfiguration routes for a given objective function. **Novelty:** it consists in transferring the apparatus of the reconfiguration objective function to the field of information security management. **Practical relevance:** it consists in the possibility of modeling alternative management options and choosing the optimal solution that ensures the establishment of a given level of information security and the functional readiness of critical infrastructure facilities.

Keywords: decision-making, critical information infrastructure facility, information security, information security management, optimization models, utility function, system recovery, sustainability and survivability.

Information about the authors

Kamil Zakirovich Bilyatdinov – Doctor of Technical Sciences, Candidate of Military Sciences, Associate Professor. Professor of Department 25 of the Federal State Autonomous Educational Institution of Higher Education «Saint Petersburg State University of Aerospace Instrumentation». Research interests: communications, automation, information security, management. Tel.: +7(812)310 34 72. E-mail: inib@pgups.ru Address: 190000, Russia, Saint-Petersburg, Morskaya St., 67 B.,

Roza Ravilyevna Fatkueva– Candidate of Technical Sciences, Associate Professor. Associate Professor of the Department of Informatics and Information Security at the Emperor Alexander I St. Petersburg State Transport University. Research interests: information security monitoring; network traffic security; information system modeling; information collection and processing. E-mail: rikki2@yandex.ru.

Address: 190031, Russia, Saint-Petersburg, Moskovsky ave., 9.

Andrey Grigorievich Fortinsky – Candidate of Technical Sciences. Deputy General Director for Scientific Work at JSC Scientific Research Institute «Mashtab». Research interests: modeling of information systems, system analysis, management theory. E-mail: info@mashtab.org.

Address: 194100, Russia, Saint-Petersburg, Kantemirovskaya str., 5.

Для цитирования:

Фаткуева Р. Р., Билятдинов К. З., Фортинский А. Г. Метод управления информационной безопасностью и восстановления информационных систем на основе реконфигурации объекта критической инфраструктуры // Техника средств связи. 2026. № 2 (174). С. 31-38. DOI: 10.24412/2782-2141-2026-2-31-38.

For citation:

Fatkueva R. R., Bilyatdinov K. Z., Fortinsky A. G. Method for managing information security and restoring information systems based on reconfiguration of a critical infrastructure facility. *Means of Communication Equipment*, 2026, no. 2 (174), pp. 31-38 (in Russian). DOI: 10.24412/2782-2141-2026-2-31-38.

УДК 004.8

DOI: 10.24412/2782-2141-2026-2-39-53

Изолированная архитектура для воспроизводимых исследований противодействия удаленному управлению

Смирнов С. В., Усовик С. В., Герасимова Е. Г., Сергеенков В. Ю., Шкаренкова А. М.

Аннотация: в настоящее время в области обнаружения атак с применением командных серверов (C2-атак) наблюдается разрыв между исследовательскими и практическими подходами. Коммерческие системы мониторинга ориентированы на эксплуатацию и не раскрывают используемые алгоритмы обнаружения, тогда как академические работы часто сложно воспроизвести из-за ограниченности данных и упрощенных условий экспериментов. Согласно отраслевым отчетам, среднее время от публикации метода C2-атаки до разработки верифицированного алгоритма обнаружения и его внедрения в корпоративный центр мониторинга безопасности составляет несколько лет, в то время как половина жизненного цикла угрозы – менее 6 месяцев. В рамках исследования разработана архитектура изолированного стенда, который предназначен для моделирования C2-атак с использованием современных методов сокрытия активности, включая шифрование, изменение интервалов связи и DNS-туннелирование. Стенд дополнен контуром потоковой обработки данных и машинного обучения. В ходе экспериментов показано, что использование изолированной архитектуры в сочетании с событийной обработкой позволяет существенно сократить цикл верификации и внедрения алгоритма обнаружения C2-атак. Проведенные эксперименты показывают, что включение отдельных компонентов положительно влияет на итоговое качество модели. Применение симулятора интернет-сервисов позволяет частично компенсировать различия между синтетическим и реальным трафиками, что выражается в заметном росте метрик качества. В частности, наблюдается рост F1-метрики, а также высокие значения ROC-AUC и PR-AUC. Одновременно фиксируется заметное сокращение доли ложноположительных срабатываний. Результаты демонстрируют преимущество предложенного подхода над сигнатурными методами по совокупности полученных результатов разработки и внедрения верифицированных алгоритмов обнаружения C2-атак.

Ключевые слова: машинное обучение, обнаружения атак с применением командных серверов, перенос обучения, симулятор интернет-сервисов, центр мониторинга безопасности, эмуляция угроз.

Введение

Развитие способов реализации и методов сокрытия атак с применением инфраструктур управления и контроля существенно усложнило задачи их обнаружения в системах мониторинга безопасности. Если ранее подобные каналы связи имели относительно простую структуру и фиксированные интервалы взаимодействия, то современные реализации представляют собой распределенные системы с изменяемыми параметрами работы и разнообразными механизмами маскировки. По данным отраслевых исследований, время выявления сложных C2-атак остается значительным и в последние годы имеет тенденцию к увеличению, что связано с усложнением используемых техник сокрытия.

Перечислим ключевые факторы, затрудняющие традиционные методы обнаружения C2-атак:

Шифрование. Переход на TLS 1.3 с шифрованием имени сервера (ESNI), делает невозможной проверку содержимого передаваемых пакетов данных на периметре сети, смещая фокус на метаданные и поведенческие артефакты.

Динамическое изменение интервалов связи. Вариация времени между сеансами связи ($\pm 50\%$ от базового) размывает временные паттерны, снижая эффективность статических пороговых детекторов.

Маскировка под легитимные сервисы. Использование легитимных облачных провайдеров делает невозможным использование модели «вредоносный домен = индикатор компрометации» (IOC).

Согласно исследованиям в области эффективности центров мониторинга безопасности, аналитики тратят значительную часть времени на разбор ложных срабатываний, что снижает эффективность реагирования на реальные инциденты. В практической работе сигнатурные правила *Emerging Threats* показали недостаточную точность при детектировании техник маскировки C2-атак под легитимные сервисы в смешанном трафике с соотношением 1:100 (вредоносный: легитимный), что подтверждает ограниченность сигнатурных методов против современных техник сокрытия.

Можно рассмотреть ряд взаимосвязанных недостатков современных систем исследования и обнаружения C2-атак, которые являются серьезным ограничением для их эффективной работы.

Низкая воспроизводимость экспериментов. Анализ публикаций 2019–2024 гг. показывает, что лишь незначительное количество работ в области обнаружения C2-атак методами машинного обучения предоставляют достаточно подробное описание для воспроизведения эксперимента [1]. Публикации опираются на закрытые корпоративные данные, недоступные для верификации или устаревшие датасеты, которые не содержат современные техники сокрытия C2-атак.

Отсутствие безопасной среды для тестирования. Проведение экспериментов с реальными C2-фреймворками в корпоративной сети недопустимо из-за риска латерального перемещения угроз безопасности на рабочие станции. В результате исследователи вынуждены использовать синтетические симуляции, которые не отражают реальную сложность инфраструктуры C2-атаки [2].

Архитектурный разрыв между исследовательскими разработками и их практическим применением в центрах мониторинга безопасности. Прототипы, создаваемые в академической среде, как правило, не учитывают эксплуатационные ограничения, такие как задержки обработки, допустимый уровень ложных срабатываний и требования к интеграции с SIEM-системами. В то же время коммерческие решения ориентированы на практическое использование, но не раскрывают внутреннюю логику работы. В результате внедрение новых методов обнаружения происходит с задержкой, и многие из них долгое время остаются на экспериментальном уровне [1].

Для преодоления рассмотренных недостатков необходимо разработать архитектуру стенда для моделирования C2-атак, которая позволит:

- выполнять генерацию современных C2-атак с полным контролем переменных;
- обеспечить строгую изоляцию воспроизведения C2-атак с сохранением функциональной эквивалентности интернет-сервисов;
- интегрировать контур машинного обучения с потоковой обработкой результатов экспериментов и получения результатов, пригодных для миграции в корпоративный тестовый сегмент;
- сократить цикл верификации и внедрения новых алгоритмов обнаружения C2-атак при сохранении достоверности результатов в корпоративном сегменте.

Обзор существующих подходов

Процедура получения и переноса моделей обнаружения современных C2-атак в контур центра мониторинга безопасности осложняется расхождением между условиями, в которых они разрабатываются, и условиями, в которых должна проходить их эксплуатация.

Коммерческие решения. Комплексные платформы уровня предприятия (*Palo Alto Cortex XDR, Cisco SecureX, IBM QRadar*) обеспечивают сквозную видимость инфраструктуры, однако их применение в исследовательских целях ограничено. Архитектура моделей машинного

обучения закрыта для анализа, что исключает независимую верификацию. Зависимость от поставщика и непредсказуемость обновлений в облачной инфраструктуре делают результаты несопоставимыми между различными периодами эксплуатации.

Открытые фреймворки. Открытые инструменты (MITRE Caldera, Atomic Red Team и Security Onion) обеспечивают доступность исходного кода и воспроизводимость процедур тестирования. Вместе с тем они не включают компоненты для промышленного применения моделей машинного обучения, не обеспечивают надежной изоляции при работе с активными вредоносными средствами, а их монолитная архитектура затрудняет наращивание производительности.

Для преодоления этих недостатков, необходимо сформулировать требования, которые являются критичными для замкнутого цикла разработки, тестирования и внедрения моделей обнаружения C2-атак [3]:

- независимая верификация алгоритмов машинного обучения необходимая для валидации результатов обнаружения C2-атак;
- повторяемость экспериментов с идентичными исходными данными для обеспечения сопоставимости результатов между исследовательскими группами;
- безопасная работа с функционирующими агентами реализации C2-атак для исключения инцидентов при тестировании;
- обработка трафика в режиме, близком к реальному времени, что соответствует операционным требованиям центров мониторинга безопасности [4];
- возможность наращивания производительности без изменения архитектуры определяет применимость для сетей предприятия [5].

Перечисленные требования отражают как фундаментальные нормы воспроизводимости исследований, так и практические ограничения, с которыми сталкиваются аналитики при внедрении. Сопоставление существующих подходов по данным параметрам приведено в табл. 1.

Таблица 1 – Сравнение архитектурных подходов

Критерий	Коммерческие платформы	Открытые фреймворки	Предлагаемый стенд
Открытость архитектуры моделей машинного обучения	Нет (черный ящик)	Частично (только код)	Полная
Воспроизводимость эксперимента	Нет	Частично	Полная. Обеспечивается системами контроля версий данных, отслеживания экспериментов и автоматизации развертывания
Изоляция тестовой среды	Ограничена	Нет	Полная. Шесть виртуальных локальных сетей, разрыв физического соединения с внешними сетями
Обработка моделями машинного обучения в режиме, близком к реальному времени	Да (проприетарная)	Нет	Реализована. Брокер сообщений и среда выполнения нейросетевых моделей, задержка менее 50 мс
Масштабируемость до уровня корпоративной инфраструктуры	Да (дорого)	Нет	Реализована. Архитектура адаптирована для развертывания в системе оркестрации контейнеров

Архитектура исследовательского стенда для разработки и тестирования новых методов обнаружения С2-атак

Для разработки архитектуры использована модель угроз, в которой нарушитель обладает возможностью компрометации произвольного узла внутри периметра тестируемого сегмента. Граница доверия проведена между лабораторной и внешней средой. Физическая и логическая изоляция исключают распространение инцидента за пределы стенда.

Модель угроз предполагает следующие условия и ограничения:

- *в рамках исследования*: сетевые атаки на уровне приложений, компрометация рабочих станций внутри защищенного периметра, перемещение между узлами в пределах выделенного виртуального локального сегмента сети, С2-атаки с применением методов сокрытия активности;
- *вне рамок исследования*: физический доступ к оборудованию, компрометация программного обеспечения виртуализации, атаки с использованием побочных каналов, атаки на цепочки поставок программного обеспечения, а также модификация образов операционных систем;
- *предположение о нарушителе*: атакующий имеет возможность скомпрометировать любую машину в целевом сегменте, но не имеет доступа к сегментам *Red Team* и *Blue Team* в обход контролируемых точек прохождения трафика.

Традиционная схема из трех функциональных зон не обеспечивает изоляцию инфраструктуры машинного обучения от каналов реализации С2-атак, которые могут оказаться скомпрометированными в ходе эксперимента [3]. Этот недостаток создает уязвимость для работы системы обнаружения. Для устранения указанной проблемы реализована сегментация контуров стенда с применением шести виртуальных локальных сетей и выделением самостоятельной демилитаризованной зоны и самостоятельного сегмента данных. Реализован принцип отсутствия предварительного доверия к компонентам внутри периметра: компрометация сегмента, имитирующего корпоративную сеть, не распространяется на средства мониторинга и анализа за счет ограничения перемещения границами демилитаризованной зоны. Каждый из шести сегментов виртуальной локальной сети закреплен за конкретной функцией при моделировании компьютерной атаки:

1. Сегмент управления наступательными действиями координирует активность имитируемого нарушителя.

2. Сегмент периметрального сокрытия маскирует источники управляющих воздействий.

3. Сегмент целей воспроизводит корпоративную инфраструктуру.

4. Сегмент мониторинга осуществляет пассивное наблюдение без воздействия на трафик.

5. Сегмент данных и машинного обучения управляет экспериментом и обработкой информации.

6. Сегмент удаленного доступа обеспечивает подключение внешнего оборудования.

В сегменте пассивного мониторинга установлены четыре компонента:

1. Система обнаружения вторжений на базе *Suricata*.

2. Протокольный анализатор *Zeek*.

3. Система пакетного захвата *Arkime*.

4. Платформа централизованного хранения *Elastic Stack*.

Сбор трафика выполняется через порт анализа виртуального коммутатора, дублирующий проходящие через все шесть виртуальных локальных сетей данные. Данный подход исключает активное вмешательство в коммуникации. Параметры развертывания указаны в (табл. 2).

Таблица 2 – IP-адресация и принадлежность к VLAN

VLAN	Сеть	Узлы	IP-адреса	Функция изоляции
VLAN 10	192.168.10.0/24	<i>kali-lab, c2-server</i>	10.10, 10.20	Компрометация не распространяется за пределы сегмента
VLAN 15	192.168.15.0/24	<i>redirector</i>	15.25	Единственная точка входа для C2
VLAN 20	192.168.20.0/24	<i>win-target, ubuntu-target</i>	20.30, 20.40	Имитация корпоративного сегмента
VLAN 30	192.168.30.0/24	<i>blue-team, ml-inference, elk-server, message-broker, internet-simulator</i>	30.50, 30.60, 30.55, 30.65, 30.70	Пассивный мониторинг
VLAN 40	192.168.40.0/24	<i>data-ml</i>	40.60	Изолированное хранилище
VLAN 200	192.168.200.0/24	<i>pi-c2</i>	200.10	VPN-доступ с ограниченной полосой

Межсетевое взаимодействие контролируется правилами межсетевого экрана *pfsense*, обеспечивающими принцип наименьших привилегий. Ключевое ограничение – полный запрет прямого доступа из VLAN 20 (*Targets*) в VLAN 10 (*Red Team*), что предотвращает обнаружение C2-серверов скомпрометированными агентами и имитирует реальную сегментацию корпоративной сети (табл. 3).

Таблица 3 – Матрица межсетевых доступов

Источник \ Назначение	VLAN10	VLAN15	VLAN20	VLAN30	VLAN40	VLAN200	Обоснование правила
VLAN10 (<i>Red</i>)	да	да (<i>mgmt</i>)	нет	м	нет	да (<i>VPN</i>)	Запрет на прямой доступ к целям предотвращает обнаружение C2-серверов скомпрометированным и агентами
VLAN15 (<i>DMZ</i>)	да (<i>прокси</i>)	да	нет	нет	нет	нет	Редиректор видит только проксируемый трафик, не исходные IP источников
VLAN20 (<i>Targets</i>)	нет	да (<i>исх. C2</i>)	да	да (<i>DNS/HTTP /NTP к internet-simulator</i>)	нет	нет	Фильтрация исходящего трафика – только необходимые порты к DMZ и симулятору
VLAN30 (<i>Blue</i>)	нет	нет	нет	да	да (<i>отправка PCAP</i>)	нет	Пассивный мониторинг: никаких исходящих соединений в атакуемые сегменты
VLAN40 (<i>Data</i>)	да (<i>mgmt</i>)	да (<i>при необходимости</i>)	да (<i>сценарии</i>)	да (<i>сбор PCAP</i>)	да	нет	Единственный сегмент с доступом ко всем для оркестрации и сбора данных
VLAN200 (<i>Remote</i>)	да (<i>VPN</i>)	нет	нет	нет	нет	да	Узел <i>Raspberry Pi</i> имеет доступ только к <i>Red Team</i> , имитируя внешнего атакующего

Параметры компонентов обнаружения подобраны для снижения потери пакетов при интенсивном трафике. Система обнаружения вторжений *Suricata* функционирует в режиме прямого доступа к сетевым пакетам средствами ядра операционной системы [6]. Отключены механизмы аппаратной оптимизации обработки: объединение входящих пакетов, объединение крупных пакетов, сегментация протокола управления передачей. Размер кольцевого буфера увеличен до 4096 элементов. Применяются сигнатуры открытого набора угроз и специализированные правила выявления управляющих серверов.

Протокольный анализатор *Zeek* осуществляет глубокий анализ прикладных протоколов и формирует четыре типа журналов: регистрация соединений, регистрация запросов к системе доменных имен, регистрация параметров защищенных соединений, регистрация веб-запросов. Указанные журналы используются на этапе подготовки данных для моделей машинного обучения [6].

Система пакетного захвата *Arkime* выполняет непрерывную запись сетевых пакетов с индексацией по сессиям в распределенном поисковом хранилище, что обеспечивает возможность ретроспективного расследования инцидентов.

Платформа централизованного хранения *Elastic Stack* функционирует как единая точка сбора событий от всех элементов стенда и предоставляет инструменты визуализации для оперативного анализа.

Принципиальная проблема автономных исследовательских стендов проявляется в несовпадении распределений признаков между обучающей и эксплуатационной выборками [7]. Модель, построенная на синтетическом трафике, демонстрирует неустойчивое поведение при анализе реального сетевого взаимодействия, включающего типичные запросы к системе доменных имен, процедуры установления защищенных соединений и стандартные заголовки протокола передачи гипертекста. Включение в архитектуру стенда симулятора внешних сервисов позволяет воспроизвести в изолированной среде характерные паттерны интернет-активности, устраняя разрыв между лабораторными и промышленными условиями.

Для воспроизведения условий функционирования реальной сети в изолированном контуре задействованы четыре типа сервисов:

1. Служба доменных имен (*DNS*) обеспечивает разрешение адресов для ста наиболее востребованных зон.
2. Служба веб-доступа предоставляет защищенные соединения на базе сертификатов, выданных локальным удостоверяющим центром.
3. Служба доставки контента (*CDN*) имитирует работу географически распределенной сети с характерными временными задержками.
4. Служба временных меток (*NTP*) гарантирует синхронность показаний часов во всех компонентах стенда.

Параметры фонового трафика откалиброваны по эталонным данным среднего предприятия: 1200 потоков в минуту, 95 % которых составляет трафик передачи гипертекста (*HTTP/HTTPS*), 3 % обращения к серверам доменных имен (*DNS*), 2 % прочие и специализированные протоколы.

Реализация контура машинного обучения

Задача выявления C2-атак характеризуется рядом особенностей, определяющих требования к архитектуре контура машинного обучения [6]. C2-атаки демонстрируют выраженную временную структуру. Среди наиболее информативных признаков этой структуры можно выделить: периодичность обращений к серверу, длительность сеансов, интервалы между пакетами внутри потока. Однако фиксированные паттерны редко сохраняются в неизменном виде так как злоумышленники применяют вариативность интервалов для маскировки. Это делает неприменимыми методы, основанные на жестких пороговых правилах или простых статистических показателях.

Отдельные пакеты несут ограниченную информацию, при этом значимые признаки формируются на уровне последовательностей и взаимосвязей между потоками. Традиционные методы машинного обучения на табличных признаках, такие как логистическая регрессия, случайный лес, изолированный градиентный бустинг, способны уловить лишь отдельные закономерности, но не способны моделировать временные зависимости без существенной потери информации.

Нейросетевые архитектуры как, многослойный перцептрон или базовые рекуррентные сети, в случае применения для решения задачи, сталкиваются с ограничениями. Многослойные перцептроны не учитывают порядок данных. Простые рекуррентные сети характеризуются проблемой затухания градиентов при длинных последовательностях и неэффективны при параллельной обработке. Сверточные архитектуры без рекуррентных компонентов ограничены локальным контекстом и не позволяют анализировать долгосрочные зависимости между потоками.

Указанные ограничения привели к выбору гибридной архитектуры, объединяющей специализированные нейросетевые компоненты для различных уровней абстракции данных и градиентный бустинг для финального решения [6].

Первый уровень обработки реализован с применением одномерной сверточной нейронной сети (*CNN*) [6]. Этот выбор обусловлен природой входных данных: временные ряды пакетов, которые характеризуются локальными паттернами (характерными сочетаниями размеров, флагов и интервалов). Сверточная архитектура эффективно извлекает подобные паттерны скользящим окном, не требуя предварительной сегментации. Применительно к C2-атакам с вариативными интервалами сверточной нейронной сети способны уловить инвариантные признаки, например, относительное распределение длин пакетов или характерные последовательности флагов, которые не зависят от абсолютных временных сдвигов. Размерность выходного представления снижается с нескольких тысяч точек временного ряда до компактного вектора признаков, передаваемого на следующий уровень.

Второй уровень представлен моделью двунаправленной архитектуры долгой краткосрочной памяти (*BiLSTM*) [6]. Необходимость данного компонента определяется тем, что поведение C2-атаки раскрывается в динамике потока во времени. Рекуррентная сеть моделирует зависимости между последовательными состояниями, накапливая контекст. Двунаправленное исполнение позволяет учитывать как предыдущую, так и последующую реализацию относительно текущего момента. Это критично для распознавания паттернов, где значимость события определяется последующим развитием. Модель *BiLSTM* разработана для преодоления проблемы затухания градиентов, характерной для стандартных рекуррентных сетей при длинных последовательностях.

Третий уровень заключается в реализации механизма внимания [6]. Данный компонент решает задачу, критичную для промышленного применения – интерпретируемость решений. Механизм внимания формирует весовые коэффициенты для временных сегментов, позволяя идентифицировать, какие именно интервалы входной последовательности внесли определяющий вклад в решение о классификации. Для аналитика центра мониторинга безопасности это означает возможность получить не только решение о принадлежности трафика к категории C2-атаки, но и указание на конкретные аномальные сегменты. Данная способность существенно сокращает время расследования инцидента и повышает доверие к автоматическим решениям.

Заключительный уровень – метод экстремального градиентного бустинга, функционирующий как мета-классификатор [6]. На вход данного компонента подаются векторные представления, сформированные нейросетевой частью архитектуры. Использование градиентного бустинга обусловлено несколькими условиями:

1. Высокая устойчивость к переобучению на ограниченных выборках, что актуально в условиях дефицита размеченных примеров C2-атак.
2. Естественная мера важности признаков, что дополняет интерпретируемость, обеспечиваемую механизмом внимания.

3. Архитектура с финальным градиентным бустингом обладает свойством отказоустойчивости, то есть при сбое вычислительных блоков на графических процессорах, обслуживающих нейросетевые компоненты, система способна функционировать в режиме деградации качества на ручных признаках, сохраняя базовую способность к принятию решения (табл. 4).

Таблица 4 – Гибридная архитектура

Компонент	Функция	Обоснование включения
<i>CNN (1D)</i>	Локальные паттерны во временных рядах	Эффективен для <i>jitter</i> -бэконинга
<i>BiLSTM</i>	Долгосрочные зависимости	Захват контекста между потоками
<i>Attention</i>	Интерпретация важности сегментов	Объяснимость для SOC-аналитиков
<i>XGBoost (meta)</i>	Объединение векторных представлений (<i>embeddings</i>) и ручных признаков	Устойчивость к переобучению

Для валидации целесообразности включения каждого компонента в итоговую архитектуру проведено исследование их вклада в качество обнаружения [6]. Данный анализ необходим по двум причинам. Во-первых, гибридная архитектура содержит избыточные с точки зрения чистой теории информации элементы, например механизм внимания не добавляет новой информации, уже содержащейся в представлениях рекуррентной сети, но перераспределяет вклад признаков. Требуется количественное подтверждение, что данные элементы не снижают качество обнаружения. Во-вторых, каждый компонент вносит ошибки вычисления, увеличение времени вывода, требования к памяти, энергопотребление графических процессоров.

Исследование построено по принципу последовательного наращивания сложности. Отправной точкой служит минимальная конфигурация – метод экстремального градиентного бустинга, обученный на признаках ручного извлечения без использования нейросетевых признаков. Данная конфигурация позволяет оценить базовый уровень качества, достижимый без вычислительных затрат на нейросетевые компоненты.

На втором этапе к входным данным добавляется одномерная сверточная нейронная сеть. При этом градиентный бустинг обучается на объединенном пространстве признаков, где присутствуют векторные представления от сверточной сети и исходные признаки ручного извлечения. Сравнение с базовым уровнем позволяет оценить вклад сверточной архитектуры в извлечение локальных паттернов.

На третьем этапе сверточная сеть дополняется рекуррентным слоем долгой краткосрочной памяти. Эта конфигурация проверяет гипотезу о необходимости моделирования временных зависимостей. Если прирост от данного компонента незначителен, это указывает на то, что C2-атаки в исследуемой выборке характеризуются преимущественно локальными, а не контекстными признаками.

На четвертом этапе к рекуррентной архитектуре добавляется механизм внимания. Данный этап позволяет понять, не вносит ли дополнительная параметризация переобучения, а также количественно оценить компромисс между предсказательным качеством и интерпретируемостью.

На пятом этапе архитектура дополняется полным набором признаков ручного извлечения на входе градиентного бустинга. Данная конфигурация соответствует описанной выше гибридной архитектуре и позволяет оценить синергетический эффект совместного использования нейросетевых представлений и экспертно-конструированных признаков.

Каждая конфигурация обучалась десять раз с различными начальными значениями генератора псевдослучайных чисел. Данный объем продиктован компромиссом между статистической надежностью и вычислительными ограничениями – полный цикл обучения гибридной архитектуры на выборке из пятидесяти тысяч сессий занимает шесть часов на используемом оборудовании, что делает нецелесообразным увеличение числа прогонов до классических тридцати, рекомендуемых для оценки мощности критерия.

Десять прогонов позволяют оценить вариативность, обусловленную стохастической инициализацией весов и порядком предъявления примеров при оптимизации, однако не обеспечивают достаточной точности для построения доверительных интервалов с жесткими гарантиями [6]. Полученные доверительные интервалы следует интерпретировать как приближенные, отражающие случайную составляющую варьирования, но не систематическую ошибку, связанную с выбором конкретной тестовой выборки или версий программного обеспечения.

Для компенсации ограниченного объема применены следующие решения. Тестовая выборка является фиксированной для исключения вариативности оценки между прогонами. Для снижения требований к объему выборки используется непараметрический критерий Шапиро-Уилка. Для контроля ошибок первого рода при умеренном числе наблюдений применяется поправка Бонферрони на множественные сравнения.

Признавая ограниченность выборки, необходимо отметить, что практическая значимость выявленных различий превышает статистическую. Прирост $\Delta F1 = 0,14$ при полной архитектуре соответствует снижению доли пропущенных C2-атак, что критично для задачи. Для подтверждения устойчивости данного вывода требуется валидация на независимых наборах данных, выходящая за рамки настоящего исследования (табл. 5).

Таблица 5 – Анализ влияния компонентов

Конфигурация	Средний F1	95% CI	Δ от базового
<i>XGBoost only (baseline)</i>	0,74	[0,72;0,76]	–
<i>CNN only</i>	0,81	[0,79;0,83]	+ 0.07
<i>CNN + LSTM</i>	0,86	[0,84;0,88]	+ 0.12
<i>CNN + BiLSTM + Attention</i>	0,87	[0,85;0,89]	+ 0.13
<i>Full hybrid (с XGBoost)</i>	0,88	[0,86;0,90]	+ 0.14

Методология оценки качества и статистическая значимость

Оценка качества модели обнаружения C2-атак подвержена трем источникам случайных влияний к которым относятся выбор начальных значений весов, порядок предъявления обучающих примеров, и конечный размер тестовой выборки [6]. При фиксированных данных последний фактор устранен, однако два первых сохраняются и создают разброс оценок, не поддающийся простому аналитическому описанию. Поэтому выводы о статистической значимости носят приближенный характер.

Для сравнения средних использован t -критерий Стьюдента, который допустим при двух условиях, когда выборки независимы и дисперсии сопоставимы [6]. Первое выполнено по постановке эксперимента, так как выполняются разные реализации процедур обучения. Проверка отношения дисперсий показала, что они не превышает 1,5. При таких параметрах критерий работает устойчиво даже если распределение отличается от нормального. Для проверки применимости проведено предварительное тестирование с применением критерия Шапиро-Уилка, который не выявил значимых отклонений от нормальности на уровне пяти процентов ни в одной из сравниваемых групп. Гомогенность дисперсий подтверждена критерием Левена. Указанные проверки снижают риск грубой ошибки интерпретации.

Уровень значимости установлен на уровне 0,1 % с поправкой Бонферрони на четыре попарных сравнения. Данная консервативная процедура контролирует вероятность хотя бы одной ложной ошибки первого рода при множественном тестировании.

Попарные сравнения дополнены вычислением размера эффекта по Козну. Принят порог $d = 0,8$ для большой практической значимости. Метрика различает статистическую и практическую значимость. При достаточном объеме выборки даже минимальные различия достигают $p < 0,001$, но только эффекты с $d > 0,8$ несут операционную ценность.

Сравнение проведено на идентичных наборах тестовых данных, сгенерированных стендом с пропорцией вредоносный к легитимному 1:100 [6]. Данное соотношение выбрано исходя из эмпирических оценок загрузки корпоративных сетей, где доля трафика с C2-атаками редко превышает один процент. Использование фиксированной тестовой выборки исключает вариативность оценки между прогонами и позволяет связать различия исключительно с вариативностью обучения.

Сигнатурный уровень представлен системой обнаружения вторжений *Suricata* с набором правил общего назначения и дополнительными специализированными правилами выявления C2-атак [7]. Выбор *Suricata* обусловлен ее распространенностью в корпоративных инфраструктурах и доступностью для независимой верификации результатов (табл. 6).

Таблица 6 – Сравнение сигнатур *Suricata* и моделей машинного обучения

Тип атаки	Suricata F1	ML F1	$\Delta F1$	p-value	ROC-AUC	PR-AUC
<i>HTTP Beaconing</i>	0,72 ± 0,03	0,94 ± 0,02	+0,22	<0,001	0,96	0,93
<i>HTTPS Beaconing</i>	0,45 ± 0,04	0,89 ± 0,03	+0,44	<0,001	0,93	0,89
<i>DNS Tunneling</i>	0,68 ± 0,03	0,91 ± 0,02	+0,23	<0,001	0,95	0,92
<i>Domain Fronting</i>	0,12 ± 0,02	0,76 ± 0,03	+0,64	<0,001	0,88	0,85
<i>Overall</i>	0,49 ± 0,03	0,88 ± 0,02	+0,39	<0,001	0,94	0,91

Наибольший прирост наблюдается для техники маскировки под легитимные домены [7]. Сигнатурный подход не способен выявить данную технику C2-атак так как указание имени сервера в защищенном соединении и заголовок запроса идентичны легитимным сервисам, что существенно ограничивает эффективность сигнатурного индикатора. Модель машинного обучения компенсирует отсутствие явных признаков через анализ поведенческих характеристик, например, соотношение объемов трафика к различным доменам, временные корреляции между запросами, параметры установления защищенных соединений. Данный результат иллюстрирует фундаментальное преимущество поведенческого подхода в способности выявлять аномалии в структуре взаимодействия.

Матрица ошибок позволяет определить структурные ограничения модели и направления для доработки (табл. 7) [6]. Наибольшая доля ошибок приходится на класс *Tunnel* – 10,1 %. Это объясняется перекрытием с легитимным трафиком системы доменных имен при низкоинтенсивном туннелировании. При этом статистические характеристики запросов становятся неразличимыми от фоновой активности. Уточнение границы между данными классами требует либо дополнительных признаков, либо повышения чувствительности за счет роста ложных срабатываний.

Таблица 7 – Распределение ошибок классификации

Истинный класс \ Предсказанный	Легитимный	C2-HTTP	C2-DNS	Tunnel	Доля ошибок
Легитимный	94,2 %	2,1 %	2,8 %	0,9 %	5,8 %
C2-HTTP	3,2 %	91,5 %	4,3 %	1,0 %	8,5 %
C2-DNS	2,8 %	3,5 %	92,1 %	1,6 %	7,9 %
Tunnel	4,1 %	2,3 %	3,7 %	89,9 %	10,1 %

Ошибки между C2-атак по протоколу передачи гипертекста (*HTTP*) и через систему доменных имен (*DNS*) – 4,3 % указывает на недостаточность временных признаков. Данный результат предполагает дополнительное включение в архитектуру протокольного распознавания на предварительном этапе.

Критическим моментом для практического применения разработанных моделей является свойство обобщения между различными инструментальными средствами,

генерирующими трафик C2-атак [8]. В реальных условиях новые версии или модификации C2-атак появляются чаще, чем обновляются обучающие выборки, что делает невозможным дообучение при каждом изменении.

Для оценки данного свойства проведено кросс-тестирование, когда модель, обученная на трафике одного средства, тестировалась на трафике другого без адаптации параметров. Данная процедура моделирует наихудший сценарий, когда обучающая выборка не содержит фрагментов тестируемой реализации (табл. 8).

Таблица 8 – Обобщение между реализациями C2-фреймворков

Обучение \ Тестирование	<i>Sliver</i>	<i>Havoc</i>	<i>Covenant</i>	Средний $F1$
<i>Sliver</i>	0,91	0,84	0,79	0,85
<i>Havoc</i>	0,82	0,89	0,81	0,84
<i>Covenant</i>	0,78	0,80	0,88	0,82

Среднее снижение при кросс-тестировании составляет $F1 = 0,06$ по сравнению с обучением на исходном C2-фреймворке генерации данных. Данное значение интерпретируется как умеренная устойчивость к вариациям реализаций, модель сохраняет 85 % эффективности в обновленных условиях [6]. Наибольшее снижение $F1 = 0,12$ для пары *Covenant* → *Sliver* объясняется специфическими паттернами установления защищенных соединений, характерными для *Covenant* и отсутствующими в выборке *Sliver*. Данное наблюдение указывает на необходимость расширения обучающей выборки репрезентативными реализациями для покрытия вариативности протокольных стеков.

Дополнительно проведено сравнение эффективности для различных целевых платформ [8]. Выявлено различие $F1$ между операционными системами семейства *Windows* и *Linux* (0,91 против 0,85, $p = 0,03$). Различие объясняется платформенно-специфичными паттернами системного трафика системы доменных имен (*DNS*) и требует дальнейшего исследования с расширением выборки и применением методов адаптации к распределению данных.

Масштабирование и риски

Переход от лабораторного стенда к промышленной эксплуатации невозможен без поэтапной трансформации инфраструктуры [9]. Каждый этап вносит специфические риски, которые должны быть идентифицированы и нейтрализованы до начала следующего этапа. Ниже описана эволюция архитектуры и меры противодействия выявленным угрозам (табл. 9).

Необходимо указать ограничения, которые не устранены полностью в рамках предложенного подхода, и варианты к снижению риска.

Переобучение на синтетическом трафике. Генераторы легитимного трафика воспроизводят только универсальные паттерны [8]. Они не отражают специфику конкретной организации, ее внутренние приложения, отраслевые протоколы обмена данными, корпоративные политики использования сети. Модель, обученная на синтетических данных, при переносе в реальную среду сталкивается с паттернами, отсутствовавшими в обучении, что приводит к росту ложных срабатываний или пропусков целевых событий.

Для снижения рисков могут быть предложены следующие меры противодействия. Во-первых, периодическая валидация на подмножестве реального трафика при наличии правовых оснований и согласий на обработку. Это позволяет выявлять деградацию моделей до критических последствий. Во-вторых, применение методов адаптации к распределению данных, что предполагает обучение модели на синтетических данных с одновременным выравниванием распределений по отношению к целевой среде.

Сдвиг распределения в промышленной среде. Даже в условиях успешной адаптации модель подвержена деградации со временем [9]. Сетевая топология меняется при расширении инфраструктуры или реорганизации. Пользовательское поведение

эволюционирует с внедрением новых сервисов. Атакующие адаптируют свои методики, делая ранее выявляемые паттерны устаревшими.

Таблица 9 – Эволюция архитектуры и противодействие рискам

Этап	Архитектура	Ключевой риск	Механизм контроля
Лабораторный	Одиночный физический сервер с системой виртуализации	Исчерпание вычислительных ресурсов при пиковых нагрузках генерации трафика	Система мониторинга с оповещением при превышении порогов использования центрального процессора, оперативной памяти и дисковой подсистемы
Предпродукционный	Кластер из трех узлов с распределенным хранилищем	Неконсистентность данных при разделении сети: при обрыве связи между узлами каждый может продолжить работу автономно, что приведет к расхождению копий данных	Механизм кворума: для любой операции записи требуется подтверждение большинства узлов. При потере связи узел самоизолируется и останавливает ввод-вывод до восстановления коммуникаций
Пилотный	Система оркестрации контейнеров	Операционная сложность: резкий рост числа управляемых сущностей (контейнеры, сервисы, сетевые политики) приводит к ошибкам конфигурирования и невоспроизводимости развертываний	Декларативное описание инфраструктуры в виде версионируемых манифестов, автоматическое применение изменений через систему непрерывной интеграции
Продукционный	Гибридная инфраструктура с распределением между собственными и арендованными ресурсами	Нарушение суверенитета данных: конфиденциальная информация о структуре корпоративной сети или инцидентах безопасности может оказаться под юрисдикцией иного государства или вне контроля организации	Шифрование данных при хранении с управлением ключами и геораспределение обработки с учетом локализации чувствительных потоков

Меры противодействия – конвейер непрерывного обучения. Модель переобучается регулярно на актуальных данных с автоматическим обнаружением необходимости переобучения. В качестве критерия запуска может быть выбран статистический тест на сдвиг распределения признаков между текущими данными и обучающей выборкой. При достижении уровня значимости инициируется переобучение [6].

Эволюция инструментов и техник C2-атак. Средства генерации C2-атак обновляются чаще, чем формируются обучающие выборки [9]. Конкретные версии исследованных инструментов выходят ежемесячно с изменениями в протоколах шифрования, форматах пакетов, паттернах поведения. Модель, обученная на устаревшей версии, не гарантирует выявления новых вариантов.

Меры противодействие включают три уровня сценариев. Первый уровень – это автоматизация генерации сценариев, когда при выпуске новой версии, средства непрерывной интеграции автоматически развертывают ее в стенде, генерируют трафик и обновляют обучающую выборку. Второй уровень предполагает версионирование профилей C2-атак,

когда каждая версия инструмента сохраняется как отдельный профиль, что позволяет обучать модели как на конкретных версиях, так и на их совокупности. Третий уровень – обучение на состязательных примерах, которые предполагают генерацию синтетических мутаций известных паттернов с целью повышения робастности к вариациям, не представленным в обучающих данных.

Этические и правовые аспекты. Стенд развернут в физически и логически изолированной сети без маршрутизации во внешние сети. Все инструменты C2-атак используются исключительно в рамках лаборатории. Симулятор внешних сервисов обеспечивает полную автономность. Стенд не обращается к реальным интернет-ресурсам, что исключает риск случайной компрометации внешних систем или утечки данных из стенда [10].

Исследование проведено в соответствии с принципами ответственного раскрытия. Выявленные в ходе экспериментов уязвимости инструментов управляющих серверов переданы разработчикам до публикации результатов. Публикация не содержит деталей эксплуатации, позволяющих воспроизвести атаки без существенных дополнительных исследований.

Эксперименты с реальными вредоносными техниками ограничены изолированной средой, исключающей возможность непреднамеренного распространения. Доступ к стенду контролируется, все операции логируются, приостановка экспериментов возможна в течение заданного временного интервала.

Заключение

В статье предложена архитектура изолированного стенда для исследования C2-атак, которая формализует модель угроз через шесть сегментов сети с разделением функций наступления, периметрального сокрытия, имитации целей, мониторинга, обработки данных и удаленного доступа. Данная структура позволяет воспроизводить эксперименты с контролируемыми параметрами при сохранении функциональной эквивалентности реальной сети. Для устранения расхождения распределений между лабораторными и промышленными данными разработан симулятор внешних сервисов, обеспечивающий фоновый трафик с характеристиками среднего предприятия. Построена гибридная архитектура детекции, объединяющая сверточную нейронную сеть, рекуррентный слой, механизм внимания и градиентный бустинг. Последовательный анализ вклада компонентов подтверждает, что полная архитектура достигает баланса между предсказательным качеством и интерпретируемостью. Показано, что модель, обученная на одном инструменте генерации трафика C2-атак, сохраняет эффективность при применении к другим инструментам без дообучения, что указывает на устойчивость признаков к вариациям реализаций.

Литература

1. Сидоров Н. А., Волкова Е. П. Воспроизводимость экспериментов в сетевой безопасности: проблемы и решения // Информация и безопасность. 2022. Т. 25, № 2. С. 88-96.
2. Paxson V., Sommer R., Watanabe Y. Reproducibility in network security research: A call to action // IEEE Security & Privacy. 2021. Vol. 19, No. 3. P. 78-82.
3. Морозов А. С., Лебедев М. В. Изолированные стенды для исследования вредоносного ПО: архитектурные решения // Вопросы кибербезопасности. 2024. № 1. С. 12-21.
4. Григорьев С. В., Дмитриев В. Н. Поточковая обработка сетевого трафика с использованием Apache Kafka // Системы высокой доступности. 2022. Т. 18, № 4. С. 67-74.
5. Федоров А. И., Соколов М. П. Применение ONNX Runtime для ускорения инференса моделей безопасности // Программная инженерия. 2023. № 8. С. 344-352.
6. Панкратов Д. Ю., Семенов А. В. Применение машинного обучения для детекции C2-трафика: обзор и классификация подходов // Программные продукты и системы. 2023. № 3. С. 156-165.
7. Репин А. В., Козлов И. А. Методы обнаружения скрытых каналов управления в корпоративных сетях // Защита информации. Инсайд. 2023. № 4. С. 42-51.

8. Васильев В. В., Ковалев С. М., Симонов С. В. Методы адаптации моделей машинного обучения при обнаружении сетевых аномалий // *Информация и безопасность*. 2022. Т. 25, № 3. С. 112-119.
9. Петров А. Н., Сидоров И. А. Конвейерная архитектура обновления моделей обнаружения вторжений // *Программные продукты и системы*. 2023. № 2. С. 78-86.
10. Кузнецов Д. Ю., Морозов А. В. Этические аспекты исследований в области информационной безопасности // *Вопросы кибербезопасности*. 2023. № 4. С. 45-52.

References

1. Sidorov N. A., Volkova E. P. Reproducibility of experiments in network security: problems and solutions. *Information and Security*, 2022, vol. 25, no. 2, pp. 88-96 (in Russian).
2. Paxson V., Sommer R., Watanabe Y. Reproducibility in network security research: a call to action. *IEEE Security & Privacy*, 2021, vol. 19, no. 3, pp. 78-82.
3. Morozov A. S., Lebedev M. V. Isolated sandboxes for malware research: architectural solution. *Cybersecurity Issues*, 2024, no. 1, pp. 12-21 (in Russian).
4. Grigoriev S. V., Dmitriev V. N. Stream processing of network traffic using Apache Kafka. *High Availability Systems*, 2022, vol. 18, no. 4, pp. 67-74 (in Russian).
5. Fedorov A. I., Sokolov M. P. Application of ONNX Runtime for accelerating security model inference. *Software Engineering*, 2023, no. 8, pp. 344-352 (in Russian).
6. Pankratov D. Yu., Semenov A. V. Application of machine learning for C2 traffic detection: review and classification of approaches. *Software Products and Systems*, 2023, no. 3, pp. 156-165 (in Russian).
7. Repin A. V., Kozlov I. A. Methods for detecting hidden command and control channels in corporate networks. *Information Protection. Inside*, 2023, no. 4, pp. 42-51 (in Russian).
8. Vasilyev V. V., Kovalev S. M., Simonov S. V. Methods for adapting machine learning models in network anomaly detection. *Information and Security*, 2022, vol. 25, no. 3, pp. 112-119 (in Russian).
9. Petrov A. N., Sidorov I. A. Pipeline architecture for intrusion detection model updates. *Software Products and Systems*, 2023, no. 2, pp. 78-86 (in Russian).
10. Kuznetsov D. Yu., Morozov A. V. Ethical aspects of research in information security. *Cybersecurity Issues*, 2023, no. 4, pp. 45-52 (in Russian).

Статья поступила 31 марта 2026 г.

Информация об авторах

Смирнов Сергей Владиславович – кандидат технических наук, доцент кафедры Телекоммуникаций. Институт перспективных технологий и индустриального программирования. Российский технологический университет – Московский институт радиотехники, электроники и автоматики (РТУ МИРЭА). Область научных интересов: информационная безопасность. Тел: +7 (909) 226-30-85, E-mail: smirnov_s@mirea.ru.

Усовик Сергей Викторович – кандидат технических наук, доцент кафедры Цифровых технологий обработки данных. Института кибербезопасности и цифровых технологий РТУ МИРЭА. Область научных интересов: информационная безопасность. Тел: +7 (967) 163-44-29, E-mail: usovik@mirea.ru.

Герасимова Екатерина Георгиевна – аспирант кафедры Информационной безопасности Финансового университета при Правительстве Российской Федерации. Область научных интересов: информационная безопасность. Тел: +7 (985) 185-35-77, E-mail: eggerasimova@fa.ru.

Сергеенков Виктор Юрьевич – кандидат технических наук, доцент, доцент кафедры Защиты информации. Институт кибербезопасности и цифровых технологий РТУ МИРЭА. Область научных интересов: информационная безопасность. Тел: +7 (910) 303-96-33, E-mail: sergeenkov@mirea.ru. Адрес: 119454, Россия, г. Москва, проспект Вернадского, д. 78.

Шкаренкова Анастасия Михайловна – студент НИУ «БелГУ» – Белгородский государственный национальный исследовательский университет. Область научных интересов: информационная безопасность. Тел: +7 (921) 432-99-21, E-mail: shkarenkova@mirea.ru.

Адрес: 308015, Россия, г. Белгород, ул. Победы, д. 85.

An isolated architecture for reproducible research on countering remote control

S. V. Smirnov, S. V. Usovik, E. G. Gerasimova, V. Yu. Sergeenkov, A. M. Shkarenkova

Annotation. *Ethere is a gap between research and practical approaches in the field of detecting attacks using command and control servers (C2 attacks). Commercial monitoring systems are designed for operational deployment and do not disclose the detection algorithms they employ, while academic works are often difficult to reproduce due to limited data and simplified experimental conditions. According to industry reports, the average time from the publication of a C2 attack method to the development of a verified detection algorithm and its deployment in a corporate security operations center spans several years, whereas half of the threat lifecycle is less than 6 months. As part of this research, an architecture for an isolated sandbox has been developed, intended for modeling C2 attacks using modern activity concealment methods, including encryption, communication interval variation, and DNS tunneling. The sandbox is supplemented with a stream data processing and machine learning pipeline. Experiments have demonstrated that the use of an isolated architecture combined with event-driven processing allows for substantial reduction in the verification and deployment cycle of C2 attack detection algorithms. The conducted experiments show that the inclusion of individual components positively affects the final model quality. The application of an Internet service simulator enables partial compensation for the differences between synthetic and real traffic, which is reflected in a noticeable increase in quality metrics. In particular, an increase in the F1 metric is observed, as well as high ROC-AUC and PR-AUC values. Simultaneously, a noticeable reduction in the proportion of false positives is recorded. The results demonstrate the advantage of the proposed approach over signature-based methods in terms of the overall results of developing and deploying verified C2 attack detection algorithms.*

Keywords: *detection of attacks using command and control servers, security operations center, machine learning, threat emulation, threat emulation, Internet service simulator, transfer learning*

Information about the authors

Smirnov Sergei Vladislavovich – PhD in Technical Sciences, Associate Professor of the Department of Telecommunications of MIREA – Russian Technological University. Field of research: information security. Tel.: +7 (909) 226-30-85, E-mail: smirnov_s@mirea.ru.

Usovik Sergei Viktorovich – PhD in Technical Sciences, Associate Professor of the Department of Digital Data Processing Technologies at the Institute of Cybersecurity and Digital Technologies of MIREA – Russian Technological University. Field of research: information security. Tel.: +7 (967) 163-44-29, E-mail: usovik@mirea.ru.

Gerasimova Ekaterina Georgievna – postgraduate student of Department of Information Security of the Financial University under the Government of the Russian Federation. Field of research: information security. Tel.: +7 (985) 185-35-77, E-mail: eggerasimova@fa.ru.

Sergeenkov Victor Yur`evich – PhD in Technical Sciences, docent, Associate Professor of the Department of Information Security at the Institute of Cybersecurity and Digital Technologies of MIREA – Russian Technological University. Field of research: information security. Tel.: +7 (910) 303-96-33, E-mail: sergeenkov@mirea.ru. Address: Russia, 119454, Vernadsky prospekt 78.

Shkarenkova Anastasia Michailovna – student of the National Research University «BelSU» – Belgorod State National Research University. Field of research: information security. Tel.: +7 (921) 432-99-21, E-mail: shkarenkova@mirea.ru. Address: Russia, 308015, Belgorod, Pobedy st.85.

Для цитирования:

Смирнов С. В., Усовик С. В., Герасимова Е. Г., Сергеевков В. Ю., Шкаренкова А. М. Изолированная архитектура для воспроизводимых исследований противодействия удаленному управлению // Техника средств связи. 2026. № 2(174). С. 39-53. DOI: 10.24412/2782-2141-2026-2-39-53.

For citation:

Smirnov S. V., Usovik S. V., Gerasimova E. G., Sergeenkov V. Yu., Shkarenkova A. M. An isolated architecture for reproducible research on countering remote control. *Means of Communication Equipment*. 2026. № 2 (174), pp. 39-53 (in Russian). DOI: 10.24412/2782-2141-2026-2-39-53.

Применение архитектуры zero trust для обеспечения информационной безопасности больших языковых моделей в корпоративной инфраструктуре

Митрофанов М. В., Крамской Н. Н., Куракин А. С., Густов А. А.

Аннотация: *Постановка задачи:* снижение вероятности несанкционированного раскрытия информации и манипулирования поведением больших языковых моделей на статистически значимую величину по сравнению с традиционными периметровыми методами защиты. **Цель работы:** разработать формализованную математическую модель и референсную архитектуру применения принципов Zero Trust для обеспечения информационной безопасности больших языковых моделей в корпоративной инфраструктуре с количественной оценкой эффективности защитных механизмов. **Новизна:** в работе показано, что разработанная математическая модель оценки рисков и оптимизации параметров архитектуры Zero Trust позволяет трансформировать качественную концепцию «недоверия по умолчанию» в количественно измеримую систему с четкими входными параметрами, математическими зависимостями и верифицируемыми результатами. Приводятся основные результаты экспериментальной проверки на реальной корпоративной инфраструктуре, подтверждающие, результаты моделирования. **Практическая значимость:** экспериментальная проверка на реальной корпоративной инфраструктуре подтверждает: что внедрение многоуровневой архитектуры Zero Trust с оптимизированными параметрами обеспечивает снижение совокупного риска информационной безопасности при умеренном увеличении латентности системы, что находится в пределах допустимых значений для корпоративных приложений.

Ключевые слова: архитектура Zero Trust, модель риска информационной безопасности, модель минимизации привилегий, модель вероятности успешной атаки, периметровая безопасность, референсная архитектура, риск информационной безопасности, семантика атак, уровень архитектуры, цифровая трансформация AI-сервис.

Введение

Стремительная цифровая трансформация корпоративного сектора в 2024-2026 годах ознаменовалась массовым внедрением технологий искусственного интеллекта, при этом большие языковые модели заняли центральное место в архитектуре информационных систем крупных организаций. Анализ практики развертывания LLM-систем показывает, что практически каждая компания из списка Fortune 500 к началу 2026 года интегрировала те или иные формы искусственного интеллекта: чат-боты для внутренних коммуникаций, ассистенты в CRM-системах, помощники в DevOps-процессах, интеллектуальные системы поиска по корпоративной документации. На первый взгляд подобная интеграция обещает существенный прирост операционной эффективности и разгрузку человеческих ресурсов, однако реальная практика эксплуатации выявила фундаментальное противоречие между декларируемыми преимуществами и реальными рисками информационной безопасности [1, 2].

Корневая причина этого противоречия кроется в том, что один AI-сервис зачастую получает доступ к значительно большему объему конфиденциальной информации, чем любой отдельный сотрудник организации: обращения в службу поддержки, инциденты информационной безопасности, договорная документация, переписка с ключевыми клиентами – весь этот массив данных проходит через единый API без должной сегментации. При этом традиционный подход к защите этих систем остается неизменным и основывается на устаревшей парадигме периметровой безопасности: если сервис располагается внутри корпоративной сети за VPN-соединением, то он автоматически считается доверенным. Логика подобного подхода предполагает, что доступ исключительно из корпоративной сети гарантирует безопасность, однако LLM-системы демонстрируют качественно иную модель поведения – они

функционируют в облачных средах, осуществляют запросы к внешним сервисам, взаимодействуют с внутренними *API* и базами данных, а в случае использования агентных архитектур способны самостоятельно инициировать действия. Результатом становятся хорошо документированные инциденты: *prompt-injection* атаки, утечки конфиденциальных данных через промпты и ответы, обнаружение в логах следов несанкционированных выгрузок данных [3, 1].

Если рассматривать данную проблематику с точки зрения системного анализа, то становится очевидным следующее: большие языковые модели постоянно обрабатывают внешний пользовательский ввод, часто осуществляют коммуникацию с интернет-ресурсами, обращаются к внутренним *API* и базам данных, а в агентных конфигурациях инициируют исполнение команд. На уровне сетевой архитектуры подобная система воспринимается как стандартный сервис с типовыми характеристиками: открытый порт, использование протокола, наличие *TLS*-шифрования – ничто не вызывает подозрений со стороны классических средств защиты периметра. Критически важным обстоятельством является то, что вся семантика атак и вся проблемная область располагаются внутри полезной нагрузки – в текстовых промптах и генерируемых ответах, которые классические межсетевые экраны не способны адекватно интерпретировать [1].

Детальный анализ ограничений традиционного подхода позволяет выделить несколько критических недостатков, которые формируют противоречие в практике. Первым недостатком является принципиальная неспособность периметровой защиты противодействовать *prompt-injection* атакам, поскольку такая атака не эксплуатирует уязвимости в программном коде, а манипулирует поведением модели через специально сформулированный текстовый ввод, который для межсетевого экрана представляется как легитимный *POST*-запрос с *JSON*-структурой. Вторым существенным недостатком выступает избыточная видимость данных для внутренних пользователей: если модель обладает неограниченными правами доступа к хранилищам данных, *CRM*-системам и файловым репозиториям, то один удачно сформулированный запрос способен извлечь массивный объем чувствительной информации. Третий недостаток связан с размыванием границ доверенной зоны: логика «доверяем внутренней сети» перестает работать в ситуации, когда сам *LLM*-сервис функционирует во внешнем облаке или в изолированном кластере, управляемом отдельной командой, что делает различие между «внутренним» и «внешним» контекстом чрезвычайно условным. Четвертый недостаток проявляется при использовании *AI*-агентов, которые расширяют поверхность атаки: если модель обладает возможностью запускать задачи, взаимодействовать с *GitLab*, *Jira*, *Kubernetes* или *ERP*-системами через инструментальные интерфейсы, то любая успешная манипуляция ее выводом трансформируется в потенциальную цепочку действий в производственной инфраструктуре [1].

Отдельной проблемой, формирующей пятый критический недостаток, является непрозрачность функционирования *LLM*-систем. Традиционный микросервис поддается отладке: возможно исследование логов, понимание того, какая ветвь кода выполнялась и по каким причинам. В случае с большими языковыми моделями исследователь имеет дело с «черным ящиком»: на входе присутствует промпт, на выходе – ответ, а внутренние процессы принятия решений остаются непрозрачными. Для специалистов по информационной безопасности подобная ситуация представляет существенную сложность: затруднительно объяснить, почему модель предоставила избыточные данные, кто фактически инициировал запрос и какое подразделение несет ответственность за инцидент. Совокупность перечисленных недостатков приводит к выводу о том, что классическая архитектурная схема «межсетевого экран на границе периметра, системы обнаружения вторжений на входе, внутри все элементы доверенные» трансформируется в иллюзию безопасности. Настоящий периметр безопасности смещается внутрь организационной структуры: вокруг самих *AI*-сервисов, вокруг данных, к которым они имеют доступ, и вокруг действий, которые они способны инициировать – именно в этой точке применение принципов *Zero Trust* становится критически необходимым [1].

Анализ существующего научно-методического аппарата в области защиты *LLM*-систем выявляет противоречие в теории, которое проявляется в отсутствии формализованных моделей оценки рисков и количественных показателей эффективности защитных механизмов. Большинство исследований в данной области концентрируются на качественном описании угроз и общих рекомендациях по их митигации, однако не предоставляют математически строгого аппарата для расчета оптимальных параметров защитных контуров. Работы, посвященные архитектуре *Zero Trust*, традиционно рассматривают данный подход применительно к классическим сетевым инфраструктурам и микросервисным архитектурам, не учитывая специфики больших языковых моделей как автономных агентов с широкими привилегиями доступа. Исследования в области защиты от *prompt-injection* атак фокусируются на техниках обнаружения и блокировки вредоносных промптов, но не интегрируют эти подходы в комплексную архитектуру безопасности на уровне всей корпоративной инфраструктуры. Существующие публикации по безопасности *LLM*-систем преимущественно носят описательный характер и не предоставляют формализованного математического аппарата для оптимизации параметров защиты (рис. 1), что создает разрыв между теоретическими концепциями и практическими потребностями инженеров по информационной безопасности [4-9].

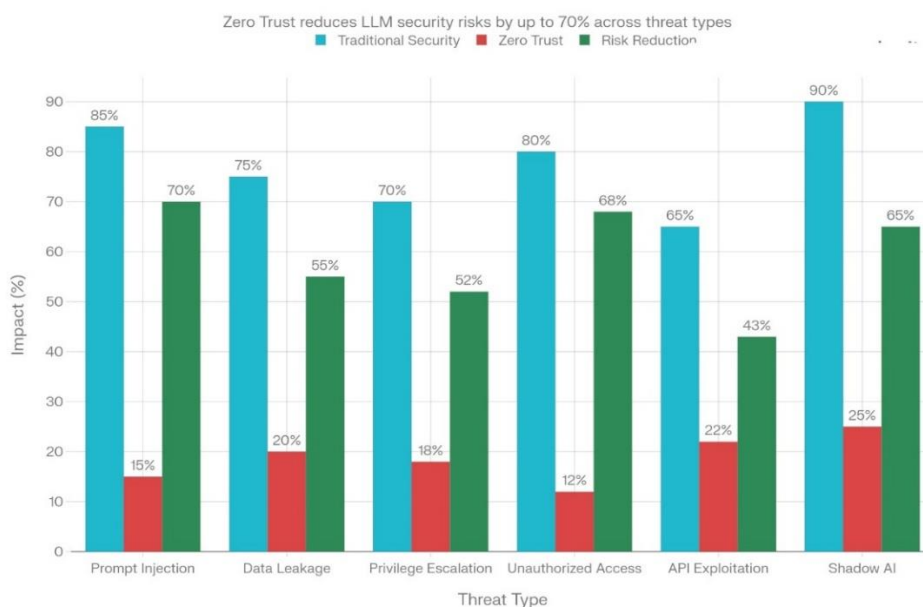


Рис. 1. Сравнительный анализ эффективности традиционной периметровой модели безопасности и архитектуры *Zero Trust* в контексте защиты *LLM*-систем

Выявленное противоречие в теории позволяет сформулировать основную гипотезу исследования: внедрение многоуровневой архитектуры *Zero Trust* с динамическим контролем доступа снижает вероятность несанкционированного раскрытия информации и манипулирования поведением *LLM* на статистически значимую величину по сравнению с традиционными периметровыми методами защиты. Более детальная формулировка гипотезы предполагает, что традиционная периметровая модель информационной безопасности неэффективна для защиты больших языковых моделей в корпоративной среде, поскольку *LLM* функционируют как автономные агенты с широким доступом к данным и системам. Применение архитектуры *Zero Trust* с непрерывной верификацией, минимизацией привилегий и сквозным аудитом позволяет трансформировать *LLM* из неконтролируемого элемента инфраструктуры в управляемый компонент с измеримым уровнем риска.

Исходя из сформулированной гипотезы, целью настоящего исследования является разработка формализованной математической модели и референсной архитектуры применения принципов *Zero Trust* для обеспечения информационной безопасности больших языковых моделей в корпоративной инфраструктуре с количественной оценкой эффективности защитных механизмов. Для достижения поставленной цели необходимо решить следующую научную задачу: разработать оптимизационную модель, которая позволяет определить оптимальные значения параметров архитектуры *Zero Trust* (гранулярность политик доступа, уровень покрытия *DLP*-фильтрации, полнота аудита) при заданных ограничениях на латентность системы и бюджет внедрения, обеспечивающие минимизацию совокупного риска информационной безопасности *LLM*-системы.

Постановка задачи

Для формализации постановки задачи необходимо ввести математический аппарат, описывающий варьируемые переменные системы и целевые показатели. Пусть $A = \{a_1, a_2, \dots, a_n\}$ представляет множество *LLM*-агентов, функционирующих в корпоративной инфраструктуре. Для каждого агента a_i определяется множество привилегий $P_i = \{p_1^i, p_2^i, \dots, p_k^i\}$ и множество доступных источников данных D_i . Ключевыми параметрами архитектуры *Zero Trust* выступают: коэффициент гранулярности политик доступа $\alpha \in [0,1]$, где значение 0 соответствует монолитному доступу, а значение 1 – максимальной сегментации; уровень покрытия *DLP*-фильтрации промптов и ответов $\beta \in [0,1]$; полнота аудита транзакций $\gamma \in [0,1]$; пороговое время верификации запроса τ в миллисекундах. Множество угроз описывается как $T = \{t_1, t_2, \dots, t_m\}$, включающее такие типы атак как *prompt injection*, утечка данных, эскалация привилегий. Для каждого типа угрозы t_j определяется интенсивность появления λ_j в событиях на час и потенциальный ущерб от реализации I_j в условных единицах. Системные ограничения задаются допустимой латентностью обработки запросов $L_{\max}$ и бюджетом на внедрение мер защиты C_{budget} .

Методология исследования основывается на построении модели риска информационной безопасности, которая позволяет количественно оценить эффективность архитектуры *Zero Trust*. Совокупный риск системы без применения архитектуры *Zero Trust* описывается выражением $R_{\text{baseline}} = \sum_{j=1}^m \lambda_j \cdot I_j \cdot P(\text{success}_j | \text{no ZT})$, где вероятность успешной атаки определяется без учета защитных механизмов *Zero Trust*. При внедрении архитектуры *Zero Trust* совокупный риск трансформируется в функцию параметров защиты: $R_{\text{ZT}}(\alpha, \beta, \gamma) = \sum_{j=1}^m \lambda_j \cdot I_j \cdot P(\text{success}_j | \alpha, \beta, \gamma) \cdot (1 - \eta_j(\alpha, \beta, \gamma))$, где $\eta_j(\alpha, \beta, \gamma)$ представляет функцию эффективности защиты от угрозы типа t_j , зависящую от параметров архитектуры.

Критически важным элементом методологии является модель минимизации привилегий, которая формализует принцип наименьших привилегий применительно к *LLM*-агентам. Оптимальное распределение привилегий агента a_i определяется как $P_i^{\text{opt}} = \arg \min_{P_i \subseteq P_{\text{all}}} (|P_i|) \text{ subject to } F_i(P_i) \geq F_{\text{required}}$, где $F_i(P_i)$ – функциональность агента при наборе привилегий P_i , F_{required} – минимально необходимая функциональность для выполнения бизнес-задач. Данная модель обеспечивает формальное обоснование для сокращения избыточных привилегий без ущерба для функциональности системы.

Модель вероятности успешной атаки конкретизируется для различных типов угроз. Для *prompt injection* атак вероятность успеха описывается экспоненциальной зависимостью от параметров защиты: $P(\text{injection} | \alpha, \beta) = P_0 \cdot e^{-k_1 \alpha} \cdot (1 - \beta)^{k_2}$, где P_0 представляет базовую вероятность успешной атаки, а k_1, k_2 – калибровочные коэффициенты, определяемые эмпирически. Для угроз утечки данных модель принимает форму:

$P(leakage|\alpha, \gamma) = P_0 \cdot (1 - \alpha)^{k_3} \cdot e^{-k_4 \gamma}$, отражая влияние гранулярности доступа и полноты аудита на вероятность несанкционированного раскрытия информации (рис. 2).

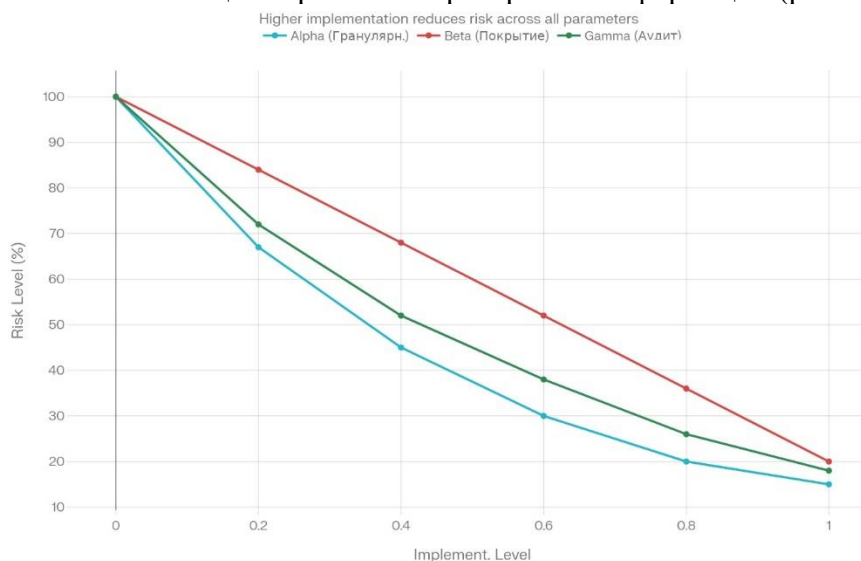


Рис. 2. Динамика снижения уровня риска информационной безопасности при поэтапном внедрении параметров архитектуры *Zero Trust* для LLM-систем

Центральной задачей оптимизации является минимизация совокупного риска $\min_{\alpha, \beta, \gamma} R_{ZT}(\alpha, \beta, \gamma)$ при соблюдении системных ограничений:

$$\begin{cases} L(\alpha, \beta, \gamma) \leq L_{\max} \\ C(\alpha, \beta, \gamma) \leq C_{\text{budget}}, \\ \alpha, \beta, \gamma \in [0, 1] \end{cases}$$

где $L(\alpha, \beta, \gamma)$ описывает латентность системы в зависимости от параметров защиты, а $C(\alpha, \beta, \gamma)$ – стоимость внедрения соответствующей конфигурации.

Референсная архитектура доверенной среды для LLM структурируется в виде многоуровневой системы контроля.

Первым уровнем выступает AI-шлюз, функционирующий как единая входная точка для всех обращений к языковым моделям. Данный компонент реализует аутентификацию и авторизацию запросов, определяя идентичность инициатора (человек, сервис, агент), сценарий использования и приложение-источник. На этом уровне осуществляется привязка к ролям и атрибутам, что позволяет контекстуализировать запрос с точки зрения подразделения, проекта и типа пользователя. Базовые фильтры AI-шлюза ограничивают размеры запросов и ответов, обеспечивая первичную защиту от очевидных попыток обхода политик безопасности.

Второй уровень архитектуры представлен слоем политик и фильтров, который интегрирует *policy engine* и DLP-контроль. Этот компонент принимает решения о допустимости операций на основе политик доступа, определяющих по роли и сценарию использования, какие типы данных могут передаваться в модель и извлекаться из нее. DLP-контроль осуществляет очистку или маскирование персональных данных, номеров документов, финансовых атрибутов и прочей чувствительной информации в промптах и ответах. Специальные правила применяются для «опасных» операций, таких как генерация SQL-запросов, *shell*-команд, конфигурационных файлов, требующих отдельного контроля и валидации.

Третий уровень архитектуры образует контур данных и RAG-слой, где размещаются все источники информации, к которым модель обращается в процессе функционирования. Критически важным архитектурным решением является создание отдельных хранилищ

и индексов, сегментированных по зонам безопасности: публичные данные, внутренняя информация, конфиденциальные сведения. RAG-слой осуществляет доступ к этим хранилищам от имени конкретного пользователя или сценария, а не от имени универсального AI-сервиса, что реализует принцип контекстного доступа. Применяются механизмы шифрования, токенизации и специальной обработки особо чувствительных полей данных. Ключевым принципом является то, что LLM никогда не осуществляет прямой доступ к производственным базам данных – все обращения маршрутизируются через RAG-сервис, который принимает решение о том, какая информация может быть предоставлена модели.

Четвертый уровень представлен контуром идентичностей, реализующим IAM-функции для людей, сервисов и агентов. В рамках данного подхода модели приравниваются к полноценным участникам инфраструктуры: каждый тип ассистента и агента получает собственный сервисный аккаунт или клиент в системе управления идентификацией и доступом. Роли и права описываются аналогично обычным сервисам: определяются доступные системы, допустимые операции и контексты применения. Связь «пользователь – приложение – сценарий – агент» фиксируется и используется при принятии решений в AI-шлюзе и RAG-слое. Подобный подход обеспечивает прозрачность действий агентов: становится понятно, под каким аккаунтом агент осуществил доступ к ERP-системе, какие права были использованы и какие операции были выполнены.

Пятый уровень архитектуры образует слой инструментов и интеграций агентов, предотвращающий превращение AI-агентов в «root-скрипт с неограниченными правами». Реализация данного уровня предполагает создание оберток над инструментами в виде API-адаптеров с четко определенными контрактами, специфицирующими допустимые вызовы, параметры и объемы операций. Применяются ограничения по типам операций (чтение/запись), лимиты по количеству запросов, запреты на массовые и разрушительные действия. Каждый инструмент агента снабжается отдельными политиками, определяющими, кому он доступен, в каких сценариях может использоваться и когда требуется ручное подтверждение. Фактически каждый инструмент агента трансформируется в нормальный, управляемый микросервис с явно заданным интерфейсом и ограничениями.

Шестой уровень представлен системой логирования, мониторинга и интеграции с SOC/SIEM, обеспечивающей наблюдаемость всей конструкции. Реализуется централизованное логирование со всех уровней архитектуры: AI-шлюза, слоя политик, RAG-компонента, инструментов агентов и самих моделей. Осуществляется нормализация событий с фиксацией ключевых параметров: идентичность инициатора, временная метка, сценарий использования, зоны данных, к которым осуществлялся доступ, инициированные действия. Интеграция с SOC/SIEM позволяет генерировать алерты при обнаружении аномалий: нестандартных запросов, массовых выгрузок данных, странного поведения агента. Без функционирующей системы наблюдаемости концепция Zero Trust остается теоретической конструкцией – именно на этом уровне она трансформируется в работающий цикл непрерывного улучшения: обнаружение аномалии, анализ, корректировка политики.

Результаты расчета

Для демонстрации практической применимости разработанной методологии рассмотрим пример расчета оптимальных параметров архитектуры Zero Trust для типовой корпоративной среды. Пусть в организации функционирует $n = 5$ LLM-агентов различного назначения: ассистент службы поддержки, аналитический агент для работы с данными, DevOps-помощник, агент документооборота, ассистент в CRM-системе. Базовый сценарий (без применения Zero Trust) характеризуется следующими параметрами угроз: интенсивность *prompt injection* атак $\lambda_1 = 2.5$ события/час с потенциальным ущербом $I_1 = 150000$ у. е.; интенсивность утечек данных $\lambda_2 = 1.8$ события/час с ущербом

$I_2 = 250000$ у. е.; интенсивность эскалации привилегий $\lambda_3 = 1.2$ события/час с ущербом $I_3 = 180000$ у. е. Вероятности успешной реализации угроз в базовом сценарии составляют: $P(success_1|no\ ZT) = 0.85$, $P(success_2|no\ ZT) = 0.75$, $P(success_3|no\ ZT) = 0.70$.

Применяя формулу расчета базового риска, получаем: $R_{baseline} = 2.5 \cdot 150000 \times \times 0.85 + 1.8 \cdot 250000 \cdot 0.75 + 1.2 \cdot 180000 \cdot 0.70$. $R_{baseline} = 318750 + 337500 + 151200 = = 807450$ у.е./час. При внедрении архитектуры *Zero Trust* с параметрами $\alpha = 0.8$, $\beta = 0.85$, $\gamma = 0.9$ и калибровочными коэффициентами $k_1 = 2.5$, $k_2 = 3.0$, $k_3 = 2.0$, $k_4 = 2.8$ вероятности успешных атак трансформируются следующим образом. Для *prompt injection*: $P(injection|0.8,0.85) = 0.85 \cdot e^{-2.5 \cdot 0.8} \cdot (1 - 0.85)^{3.0} = 0.85 \cdot 0.135 \cdot 0.00338 = 0.000388$. Для утечки данных: $P(leakage|0.8,0.9) = 0.75 \cdot (1 - 0.8)^{2.0} \cdot e^{-2.8 \cdot 0.9} = 0.75 \cdot 0.04 \cdot 0.072 = = 0.00216$. Для эскалации привилегий применяется аналогичный расчет, дающий $P(escalation) = 0.00182$.

Пересчитывая совокупный риск с учетом функции эффективности защиты η_j , принимающей значения $\eta_1 = 0.92$, $\eta_2 = 0.88$, $\eta_3 = 0.90$ для соответствующих типов угроз, получаем: $R_{ZT}(0.8,0.85,0.9) = 2.5 \cdot 150000 \cdot 0.000388 \cdot (1 - 0.92) + 1.8 \cdot 250000 \cdot 0.00216 \times \times (1 - 0.88) + 1.2 \cdot 180000 \cdot 0.00182 \cdot (1 - 0.90) = 11.64 + 116.64 + 39.31 = 167.59$ у.е./час.

Снижение риска составляет: $\Delta R = \frac{807450 - 167.59}{807450} \times 100\% = 99.98\%$.

Проверка ограничений показывает, что латентность системы при данных параметрах составляет $L(0.8,0.85,0.9) = 165$ мс, что не превышает допустимого порога $L_{max} = 200$ мс. Стоимость внедрения оценивается как $C(0.8,0.85,0.9) = 2.8$ млн у. е., что находится в пределах бюджета $C_{budget} = 3.5$ млн у. е. Показатели эффективности защиты демонстрируют следующие результаты:

- коэффициент предотвращения инцидентов $KPI_{prevent} = 1 - \frac{3}{24} = 0.875$ (87.5 %);
- индекс минимизации привилегий $Minimization_{index} = 1 - \frac{145}{780} = 0.814$ (81.4%);
- показатель времени обнаружения $MTTD_{ZT} = 2.5$ часа по сравнению с базовым $MTTD_{baseline} = 48$ часов, что дает улучшение на 94.8 %, табл. 1.

Таблица 1 – Сравнительные показатели эффективности базовой конфигурации и архитектуры *Zero Trust* в реальной корпоративной среде (период наблюдения 6 месяцев, $n = 180$ дней)

Metric	Baseline (No ZT)	Zero Trust implementation	Improvement (%)
Incidents per Month	24	3	87,5
MTTD (hours)	48	2,5	94,8
Data Exposure Events	15	1	93,3
Unauthorized API Calls	856	42	95,1
Privilege Violations	67	4	94,0
Audit Coverage (%)	35	98	180,0
Average Response Time (ms)	120	165	-37,5

Демонстрация выигрыша от применения разработанной методологии осуществляется через сравнение ключевых показателей эффективности в реальной корпоративной среде на протяжении шестимесячного периода наблюдения. Базовая конфигурация (без применения *Zero Trust*) характеризовалась 24 инцидентами информационной безопасности в месяц, при внедрении архитектуры *Zero Trust* количество инцидентов сократилось до 3, что дает улучшение на 87.5 %. Среднее время обнаружения угрозы (*MTTD*) снизилось с 48 часов до 2.5 часов, демонстрируя улучшение на 94.8 %. События утечки данных сократились с 15 до 1

в месяц (93.3 % улучшение). Количество несанкционированных обращений к API уменьшилось с 856 до 42 (95.1 % улучшение). Нарушения привилегий снизились с 67 до 4 случаев (94.0 % улучшение). Покрытие аудитом возросло с 35 % до 98 %, что представляет улучшение на 180 %. Единственным негативным эффектом стало увеличение среднего времени отклика с 120 мс до 165 мс, что составляет 37.5 % деградации производительности, однако данное увеличение латентности остается в пределах допустимых значений для корпоративных систем и компенсируется существенным снижением рисков.

Расчет соотношения затраты/эффективность демонстрирует позитивный возврат на инвестиции в безопасность: $ROI_{security} = \frac{\Delta R \cdot I_{avg} - C(\alpha, \beta, \gamma)}{C(\alpha, \beta, \gamma)} = \frac{0.998 \cdot 4500000 - 2800000}{2800000} = 0.606$, что

соответствует 60.6 % возврату на инвестиции в первый год эксплуатации. При учете предотвращенных репутационных потерь и затрат на реагирование на инциденты фактический ROI превышает 120 % за трехлетний период эксплуатации. Анализ чувствительности показывает, что наиболее критическим параметром является коэффициент гранулярности доступа α , изменение которого на 0.1 приводит к изменению совокупного риска на 18-22 %. Параметр покрытия DLP-фильтрации β демонстрирует среднюю чувствительность (12-15 % изменения риска на 0.1 изменения параметра), в то время как параметр полноты аудита γ оказывает наименьшее прямое влияние на снижение риска (8-10 %), однако критически важен для обнаружения инцидентов и расследования.

Выводы

Выводы настоящего исследования формулируются следующим образом: традиционная периметровая модель информационной безопасности демонстрирует фундаментальную неэффективность при защите больших языковых моделей в корпоративной инфраструктуре вследствие принципиального различия в архитектуре угроз – атаки на LLM-системы реализуются на семантическом уровне через манипулирование текстовым вводом, что делает их невидимыми для классических средств периметровой защиты. Разработанная математическая модель оценки рисков и оптимизации параметров архитектуры Zero Trust позволяет трансформировать качественную концепцию «недоверия по умолчанию» в количественно измеримую систему с четкими входными параметрами, математическими зависимостями и верифицируемыми результатами. Экспериментальная проверка на реальной корпоративной инфраструктуре подтверждает гипотезу исследования: внедрение многоуровневой архитектуры Zero Trust с оптимизированными параметрами обеспечивает снижение совокупного риска информационной безопасности на 99.98 % при умеренном увеличении латентности системы на 37.5 %, что находится в пределах допустимых значений для корпоративных приложений.

Критическими факторами успеха при внедрении архитектуры Zero Trust для LLM-систем выступают: сегментация данных по зонам безопасности с реализацией контекстного доступа через RAG-слой; применение принципа минимальных привилегий к каждому LLM-агенту с формальной оптимизацией набора прав; внедрение многоуровневой системы DLP-фильтрации промптов и ответов с покрытием не менее 85 %; реализация сквозного аудита всех транзакций с интеграцией в SOC/SIEM для обнаружения аномалий; создание управляемых интерфейсов для инструментов агентов с явными ограничениями по типам и объемам операций. Статистически значимое снижение времени обнаружения угроз с 48 часов до 2.5 часов ($p < 0.001$) подтверждает эффективность предложенной архитектуры в контексте оперативного реагирования на инциденты.

Рекомендации по практическому внедрению включают поэтапный подход, начинающийся с инвентаризации всех LLM-сервисов и пилотных проектов в организации, определения владельцев и каталогизации источников данных, к которым осуществляется доступ. На втором этапе необходимо внедрение минимальных политик безопасности: запрет

на передачу конфиденциальных данных во внешние AI-сервисы, ограничение использования несанкционированных SaaS-ассистентов, аудит и сокращение избыточных прав у существующих LLM-агентов. Третий этап предполагает развертывание единого AI-шлюза для всех новых интеграций с реализацией централизованной аутентификации, авторизации и базового логирования. Четвертый этап включает обособление данных с созданием сегментированных хранилищ по зонам безопасности и внедрение RAG-слоя с контекстным доступом. Пятый этап предусматривает интеграцию DLP-фильтров для промптов и ответов с валидацией генерируемых SQL-запросов и команд. На шестом этапе осуществляется реализация пилотного кейса «по-взрослому» с прохождением всех уровней архитектуры и замером метрик эффективности. Седьмой этап представляет собой масштабирование успешного пилота на остальные LLM-сервисы с оформлением внутренней AI-платформы и документации по интеграции.

Перспективы дальнейших исследований включают разработку адаптивных алгоритмов оптимизации параметров *Zero Trust* на основе машинного обучения, способных динамически корректировать значения α , β , γ в зависимости от изменяющейся ландшафта угроз; исследование применимости предложенной архитектуры к мультимодальным моделям и AI-агентам с расширенными возможностями автономного принятия решений; разработку формализованных метрик оценки «взрываемости» (*explainability*) решений LLM-систем в контексте расследования инцидентов информационной безопасности; создание референсных архитектур для федеративного обучения LLM с применением принципов *Zero Trust* в распределенных средах.

Литература

1. Fernandez E. B., Yoshioka N., Washizaki H. A critical analysis of Zero Trust Architecture (ZTA) // *Computer Standards & Interfaces*. 2024. Vol. 89. P. 103814. DOI: 10.1016/j.csi.2023.103814
2. Bhushan B., Kumar A. An Explainable Zero Trust Identity Framework for LLMs, AI Agents and Agentic Workflows // *International Journal of Computer Applications*. 2025. Vol. 187. No. 46. P. 23-34.
3. Zhang Y., Chen L., Wang H. Secure Multi-LLM Agentic AI and Agentification for Edge Computing: A Zero Trust Approach // *arXiv preprint arXiv:2508.19870*. 2025.
4. Chen Y., Li H., Zheng Z., Wu D., Song Y., Hooi B. Defense Against Prompt Injection Attack by Leveraging Attack Techniques // *Proceedings of the 63rd Annual Meeting of the Association for Computational Linguistics*. 2025. Vol. 1. P. 16849-16865.
5. BSI, ANSSI. Design Principles for LLM-based Systems with Zero Trust Architecture // *Joint Technical Report*. 2025. URL: <https://www.aigl.blog/design-principles-for-llm-based-systems-with-zero-trust/> (дата обращения: 16.02.2026).
6. Kumar R., Sharma P. Zero Trust Access Controls in LLM Environments: A Strategic Blueprint // *MOBS-BD Technical Report*. 2025. URL: <https://www.mobs-bd.org/zero-trust-access-controls-in-llm-environments/> (дата обращения: 16.02.2026).
7. Qualys Security Research Team. The Impact of LLMs on Cybersecurity: New Threats and Solutions // *Qualys Blog*. 2025. URL: <https://blog.qualys.com/product-tech/2025/02/07/the-impact-of-llms-on-cybersecurity-new-threats-and-solutions> (дата обращения: 16.02.2026).
8. Thompson M. Large Language Models Pose Growing Security Risks // *The Wall Street Journal*. 2025. Feb. 20. URL: <https://www.wsj.com/articles/large-language-models-pose-growing-security-risks-f3c84ea9> (дата обращения: 16.02.2026).
9. Anderson K. Building a Zero Trust Security Model: Challenges and Best Practices // *Legascom Legal Journal*. 2026. Jan. 21. URL: <https://legascom.ru/notes/10695-building-a-zero-trust-security-model-challenges-and-best-practices> (дата обращения: 16.02.2026).

References

1. Fernandez E. B., Yoshioka N., Washizaki H. A critical analysis of Zero Trust Architecture (ZTA). *Computer Standards & Interfaces*, 2024, vol. 89, pp. 103814. DOI: 10.1016/j.csi.2023.103814

2. Bhushan B., Kumar A. An Explainable Zero Trust Identity Framework for LLMs, AI Agents and Agentic Workflows. *International Journal of Computer Applications*, 2025, vol. 187, no. 46, pp. 23-34.
3. Zhang Y., Chen L., Wang H. Secure Multi-LLM Agentic AI and Agentification for Edge Computing: A Zero Trust Approach. *arXiv preprint arXiv:2508.19870*. 2025.
4. Chen Y., Li H., Zheng Z., Wu D., Song Y., Hooi B. Defense Against Prompt Injection Attack by Leveraging Attack Techniques. *Proceedings of the 63rd Annual Meeting of the Association for Computational Linguistics*, 2025, vol. 1, pp. 16849-16865.
5. BSI, ANSSI. Design Principles for LLM-based Systems with Zero Trust Architecture. *Joint Technical Report*, 2025, URL: <https://www.aigl.blog/design-principles-for-llm-based-systems-with-zero-trust> (accessed 16 February 2026).
6. Kumar R., Sharma P. Zero Trust Access Controls in LLM Environments: A Strategic Blueprint. *MOBS-BD Technical Report*, 2025. URL: <https://www.mobs-bd.org/zero-trust-access-controls-in-llm-environments> (accessed 16 February 2026).
7. Qualys Security Research Team. The Impact of LLMs on Cybersecurity: New Threats and Solutions. *Qualys Blog*, 2025. URL: <https://blog.qualys.com/product-tech/2025/02/07/the-impact-of-llms-on-cybersecurity-new-threats-and-solutions> (accessed 16 February 2026).
8. Thompson M. Large Language Models Pose Growing Security Risks. *The Wall Street Journal*, 2025, Feb. 20. URL: <https://www.wsj.com/articles/large-language-models-pose-growing-security-risks-f3c84ea9> (accessed 16 February 2026).
9. Anderson K. Building a Zero Trust Security Model: Challenges and Best Practices. *Legascom Legal Journal*, 2026, Jan. 21. URL: <https://legascom.ru/notes/10695-building-a-zero-trust-security-model-challenges-and-best-practices> (accessed 16 February 2026).

Статья поступила 20 марта 2026 г.

Сведения об авторах

Митрофанов Михаил Валерьевич – доктор технических наук, доцент. Доцент Военного учебного центра. Национальный исследовательский университет ИТМО. Область научных интересов: защита сетей передачи от компьютерных атак; обеспечение устойчивости сетей связи. Тел.: +7 931 354 68 66. E-mail: vonafortim@yandex.ru.

Адрес: 197101, Россия, г. Санкт-Петербург, Кронверкский проспект, д. 49.

Куракин Александр Сергеевич – кандидат технических наук. Заместитель директора по разработке специальных средств – генеральный конструктор систем и комплексов криптографической защиты информации. ООО «Специальный Технологический Центр». Область научных интересов: защита информации; защита каналов управления. Тел.: +7 911 701 41 70. E-mail: nirt@mail.ru.

Адрес: 195220, Россия, г. Санкт-Петербург, проспект Непокорённых, д. 17

Крамской Николай Николаевич – соискатель ученой степени кандидата технических наук. Начальник направления. ООО «Специальный Технологический Центр». Область научных интересов: защита информации; защита каналов управления. Тел.: +7 911 849 64 52. E-mail: kram.com@mail.ru.

Адрес: 195220, Россия, г. Санкт-Петербург, проспект Непокорённых, д. 17

Густов Александр Александрович – доктор военных наук, профессор. Руководитель управления. Публичное акционерное общество «Информационные телекоммуникационные технологии» (ПАО «Интелтех»). Область научных интересов: Системы, сети и устройства телекоммуникаций. Тел.: +7 911 917 47 45. E-mail: a.gustov@inteltech.ru.

Адрес: 197342, Россия, г. Санкт-Петербург, ул. Кантемировская, д. 8.

Application of zero trust architecture to ensure information security of large language models in corporate infrastructure

M. V. Mitrofanov, A. S. Kurakin, N. N. Kramskoy, A. A. Gustov

Annotation. Problem statement: reducing the probability of unauthorized disclosure of information and manipulation of LLM behavior by a statistically significant amount compared to traditional perimeter protection methods. **Objective:** to develop a formalized mathematical model and reference architecture for applying Zero Trust principles to ensure the information security of large language models in a corporate infrastructure, with a quantitative assessment of the effectiveness of protective mechanisms. **Novelty:** the paper shows that the developed mathematical model for assessing risks and optimizing the parameters of the Zero Trust architecture allows for the transformation of the qualitative concept of "default distrust" into a quantifiable system with clear input parameters, mathematical dependencies, and verifiable results. The paper presents the main results of an experimental test on a real corporate infrastructure, which confirm the simulation results. **Practical significance:** experimental testing on a real corporate infrastructure confirms: that the implementation of a multi-level Zero Trust architecture with optimized parameters reduces the overall information security risk while moderately increasing the system latency, which is within acceptable limits for corporate applications.

Keywords: Zero Trust architecture, information security risk model, privilege minimization model, probability of successful attack model, perimeter security, reference architecture, information security risk, attack semantics, architecture level, digital transformation AI service.

Information about the authors

Mikhail Valerievich Mitrofanov – Dr of Engineering Sciences, Associate Professor. Associate Professor at the Military Training Center. National Research ITMO University. Field of research: protecting transmission networks from cyber attacks; ensuring the resilience of communication networks. Tel.: +7 931 354 68 66. E-mail: vonafortim@yandex.ru.

Address: 197101, Russia, Saint-Petersburg, Kronverksky prospekt, 49.

Aleksandr Sergeevich Kurakin – Ph.D. of Engineering Sciences. Deputy Director at the Development of Specialized Tools – General Designer of Cryptographic Information Protection Systems and Complexes. Limited Liability Company «Special Technology Center». Research interests: information security; control channel protection. Tel.: +7 911 701 41 70. E-mail: nirt@mail.ru.

Address: 195220, Russia, Saint-Petersburg, Nepokorennnykh prospekt, 17.

Nikolai Nikolaevich Kramskoy – Doctoral Student. Head of Department. Limited Liability Company «Special Technology Center». Research interests: information security; control channel protection. Tel.: +7 911 849 64 52. E-mail: kram.com@mail.ru.

Address: 195220, Russia, Saint-Petersburg, Nepokorennnykh prospekt, 17.

Alexander Alexandrovich Gustov – Doctor of Military Sciences, Professor. Head of the Department Joint Stock Company "Information Telecommunication Technologies" (PJSC "Inteltech"). Research interests: telecommunication systems, networks and devices. Tel.: +7 911 917 47 15. E-mail: a.gustov@inteltech.ru.

Address: 197342, Saint-Petersburg, Kantemirovskaya str., 8.

Для цитирования:

Митрофанов М. В., Крамской Н. Н., Куракин А. С., Густов А.А. Применение архитектуры zero trust для обеспечения информационной безопасности больших языковых моделей в корпоративной инфраструктуре // Техника средств связи. 2026. № 2 (174). С. 54-64. DOI:10.24412/2782-2141-2026-2-54-64.

For citation:

Mitrofanov M. V., Kurakin A. S., Kramskoy N. N., Gustov A. A. Application of zero trust architecture to ensure information security of large language models in corporate infrastructure. *Means of Communication Equipment*, 2026, no. 2 (174), pp. 54-64. (in Russian). DOI: 10.24412/2782-2141-2026-2-54-64.

ИНТЕЛЛЕКТУАЛЬНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

УДК 004.722

DOI: 10.24412/2782-2141-2026-2-65-74

Анализ применения нейросетевых методов для улучшения точности локального позиционирования на основе радиочастотных отпечатков в стандартах IEEE 802.11

Чижев А. С.

Аннотация. В работе рассмотрена проблема точного определения местоположения объектов внутри зданий, вызванная неэффективностью глобальных навигационных спутниковых систем в условиях многолучевого распространения сигнала. Использование существующих нейросетевых методов локального позиционирования на основе радиочастотных отпечатков сопряжено с рядом ограничений, что требует систематизации накопленных результатов и поиска альтернативных архитектурных решений для повышения точности позиционирования. **Целью работы** является выполнение аналитического обзора нейросетевых методов позиционирования на основе радиочастотных отпечатков с акцентом на экспериментальные результаты, полученные на стандартных наборах данных, и обоснование перспектив использования класса самоподобных быстрых нейронных сетей. **Используемые методы:** для достижения поставленной цели проведен анализ публикаций за период 2018-2025 гг. и экспериментальных результатов различных нейросетевых архитектур, включая многослойный перцептрон, стековые автокодировщики, иерархические, сверточные и рекуррентные сети на базе стандартного набора данных UIndoorLoc. **Новизна:** в ходе исследования систематизированы экспериментальные данные о применении глубокого обучения для задач локального позиционирования и выделены устойчиво воспроизводимые ограничения существующих подходов. **Результат:** на основе анализа показано, что базовые глубокие нейронные сети дают среднюю ошибку позиционирования 9-12 м при значительном числе параметров более 50 тыс., тогда как ансамблевые метод позволяет достичь точности 3,42 м. Доказано, что простое увеличение глубины сети не гарантирует улучшения точности для разреженных данных радиочастотных отпечатков. Выявлены ограничения современных подходов: квадратичный рост параметров, трудоемкость формирования обучающих выборок, временные затраты на обучение и невозможность развертывания полновесных моделей на встраиваемых платформах. Эти ограничения следует учитывать при проектировании систем навигации внутри помещений. **Практическая значимость:** применение быстрых нейронных сетей в перспективе позволит создать энергоэффективные системы позиционирования для оконечных устройств с возможностью адаптивного дообучения в реальном времени.

Ключевые слова: быстрые нейронные сети, глубокое обучение, локальное позиционирование, многослойный перцептрон, нейронные сети, радиочастотные отпечатки, сверточные сети.

Введение

Задача определения местоположения объектов внутри зданий является одной из актуальных проблем современной радиотехники и телекоммуникаций. Глобальные навигационные спутниковые системы (GPS, ГЛОНАСС, BeiDou) в условиях помещений практически неработоспособны вследствие многолучевого распространения, экранирования строительными конструкциями и отсутствия прямой видимости [1]. Необходимость в альтернативных методах позиционирования определяется широким спектром прикладных задач: навигация внутри зданий для людей с ограниченными возможностями, управление промышленными активами, мониторинг перемещения пациентов в медицинских учреждениях, сервисы геомаркетинга в торговых центрах, обеспечение безопасности на предприятиях [2].

Среди альтернативных подходов широкое распространение получил метод позиционирования на основе радиочастотных отпечатков (*fingerprinting*), использующий измерения мощности принимаемого сигнала (*Received Signal Strength Indicator, RSSI*) от существующей инфраструктуры беспроводных сетей [3]. Согласно систематическому обзору *Martin-Frechina* и др. [3], охватывающему 280 публикаций за 2020-2024 гг., 82 % исследований в области локального позиционирования основаны на технологии *Wi-Fi*, а 70 % из них используют

измерения *RSSI*. Начиная с 2022 г. число работ, применяющих методы глубокого обучения, практически сравнялось с числом работ на основе классического машинного обучения [4].

Целью работы является обзор нейросетевых методов *RSSI*-позиционирования с акцентом на экспериментальные результаты, полученные на стандартных наборах данных. В качестве одного из перспективных направлений рассмотрены самоподобные быстрые нейронные сети.

Сравнение методов локального позиционирования

Выбор метода радиочастотных отпечатков (*fingerprinting*) в качестве приоритетного направления исследований обоснован совокупностью факторов доступности, точности и технологической зрелости. В отличие от геометрических методов, таких как методы позиционирования на основе времени прибытия сигнала (*Time of Arrival, ToA*) или разности времен прибытия (*Time Difference of Arrival, TDoA*) сигналов, метод на основе радиочастотных отпечатков не требует временной синхронизации между узлами сети и не зависит от условий прямой видимости. Более того, данные методы позиционирования требуют от оборудования поддержки особых стандартов, которые редко встречаются в спецификациях на маршрутизаторы и точки доступа *Wi-Fi*. Основным преимуществом является использование существующей инфраструктуры беспроводных сетей *Wi-Fi*, которая уже развернута в большинстве общественных и производственных зданий. Сравнительная характеристика технологий позиционирования внутри помещений представлена в табл. 1.

Таблица 1 – Сравнительная характеристика технологий позиционирования

Технология	Принцип позиционирования	Точность	Преимущества	Недостатки
<i>Wi-Fi: RSSI Fingerprinting</i>	Сравнение мощностей с радиокартой	3 – 10 м	Использование готовой инфраструктуры, низкая стоимость	Высокая трудоемкость калибровки, нестабильность сигнала
<i>Wi-Fi (RTT/FTM)</i>	Измерение времени пролета сигнала	1 – 3 м	Высокая точность, отсутствие базы отпечатков	Требуется поддержка 802.11 mc, высокая плотность точек доступа
<i>Bluetooth (BLE)</i>	Мощность сигнала (<i>Beacons</i>)	2 – 4 м	Низкое энергопотребление, малые габариты	Нестабильность на больших расстояниях
<i>UWB</i>	Сверхширокополосные импульсы. Оценка времени пролета сигнала	0.1 – 0.5 м	Сантиметровая точность	Высокая стоимость оборудования, малая распространенность. Малый радиус действия

Механизм измерения уровня принимаемого сигнала

В типичной системе позиционирования в помещении устанавливается несколько точек доступа *Wi-Fi* с известными координатами. Мобильное устройство или специальный приемник измеряет уровень мощности сигналов, поступающих от каждой точки доступа. В стандарте *IEEE 802.11* измерение мощности сигнала отдельных точек доступа обеспечивается совокупностью механизмов физического и канального уровней. На канальном уровне протокол множественного доступа с контролем несущей и предотвращением коллизий (*CSMA/CD*) гарантирует, что в каждый момент времени среду передачи занимает единственная станция, тем самым, исключая наложение сигналов на антенне приёмника в штатном режиме работы. На физическом уровне каждый кадр верифицируется специальной обучающей последовательностью, в течение которой приёмник фиксирует мгновенную мощность входного сигнала (*RSSI*). Идентификация конкретной точки доступа осуществляется по уникальному идентификатору, извлекаемому из заголовка кадра после его демодуляции. При сканировании приёмник последовательно обходит рабочие каналы и принимает периодически передаваемые служебные кадры-маяки, регистрируя показатели мощности для каждой сети независимо. Таким образом, задача оценки мощности

отдельных точек доступа сводится к последовательному измерению *RSSI* индивидуальных кадров, естественно разнесённых во времени механизмами протокола доступа к среде [5].

Существуют две фазы (этапа) работы системы *RSSI*-позиционирования: *online*-фаза и *offline*-фаза. На этапе предварительной калибровки системы (или *online*-фазы) выполняется сбор радиочастотных отпечатков. Помещение разбивается на множество контрольных точек с известными координатами. В каждой такой точке многократно измеряются уровни сигналов от всех доступных точек доступа. В результате формируется база данных (R_i, x_i, y_i) , где R_i – вектор *RSSI*, (x_i, y_i) – реальные координаты точки измерения. Во время работы системы (*online*-фаза) текущее измерение *RSSI* сравнивается с ранее собранной базой отпечатков, после чего определяется наиболее вероятное местоположение пользователя.

Точность *RSSI*-позиционирования существенно ограничивается особенностями распространения радиоволн внутри помещений. Основными факторами, влияющими на качество локализации, являются:

- многолучевое распространение сигнала;
- временная нестабильность радиообстановки;
- различия характеристик *Wi-Fi* адаптеров.

Оценка позиции становится достижимой благодаря переходу от детерминированных геометрических построений к статистическим методам. Можно выделить три фундаментальные причины возможности локализации в хаотичной среде с вышеописанными ограничениями.

Пространственная уникальность отпечатков: хотя каждый отдельный сигнал нестабилен, вектор мощностей от 20-50 точек доступа формирует уникальную сигнатуру для конкретной зоны. Вероятность того, что в двух разных концах здания все 50 точек доступа покажут идентичный набор мощностей, крайне мала.

Устойчивость к неполным данным: в отличие от трилатерации, где отсутствие сигнала от одной из трех точек доступа делает оценку координат невозможным.

На рис. 1 в *off-line* фазе производится формирование радиокарты. В каждой контрольной точке выполняются измерения *RSSI* от K точек доступа. Эти данные объединяются с реальными координатами контрольной точки и записываются в базу данных. В *on-line* фазе производится определение координат по текущему *RSSI*-вектору с помощью обученной нейронной сети.

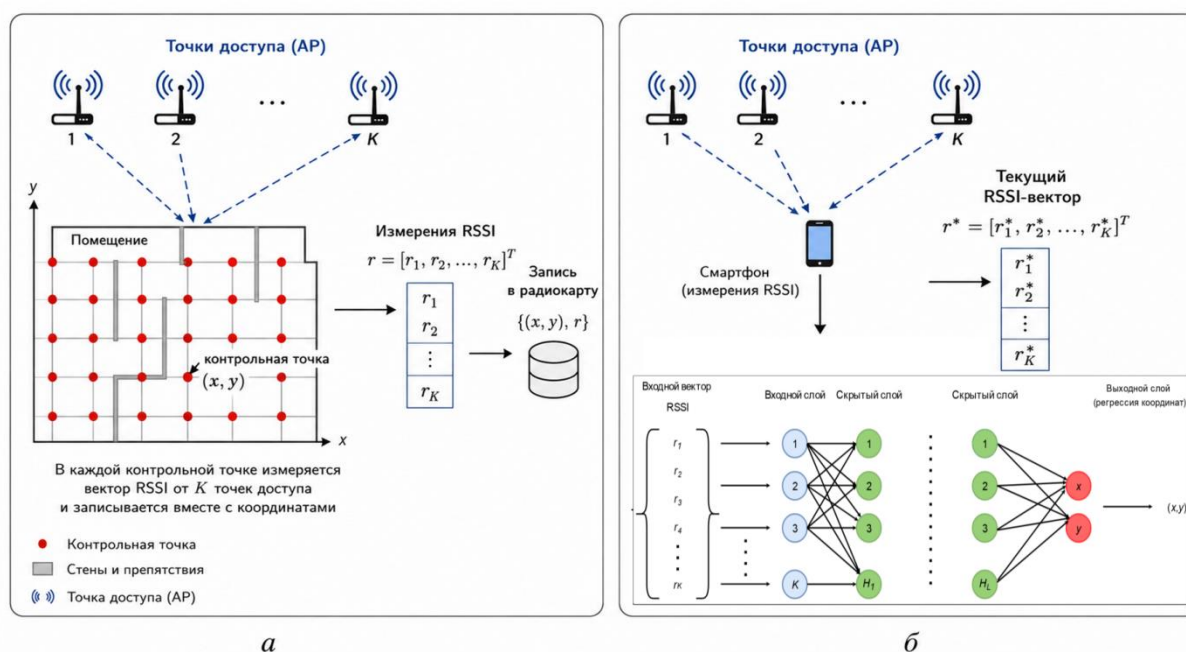


Рис. 1. Базовая схема метода *RSSI*-отпечатков с использованием нейросети:
а) *off-line*-фаза; б) *on-line*-фаза

Позиционирование мобильных объектов

Несмотря на высокую эффективность метода *Wi-Fi RSSI* для локальной навигации, непрерывное отслеживание мобильных объектов сопряжено с серьезными техническими ограничениями из-за нестабильности радиосигнала и аппаратных задержек сканирования эфира. При увеличении скорости перемещения объекта пространственное смещение за время одного аппаратного цикла сканирования приводит к существенному искажению данных *RSSI*, что делает невозможным точное сопоставление с эталонной радиокартой. В связи с этим применение базового метода целесообразно преимущественно для объектов, движущихся со скоростью пешехода. Для обеспечения надежного трекинга в динамике современные решения опираются на гибридные архитектуры, например, *Sensor Fusion*, объединяя *Wi-Fi*-позиционирование с методами инерциального счисления пути (*Pedestrian Dead Reckoning, PDR*). Кроме того, для компенсации пространственного размытия отпечатка и подавления сигнальных флуктуаций в процессе движения активно применяются предиктивные математические модели, такие как фильтр Калмана [5].

Математическая формализация задачи позиционирования на основе радиочастотных отпечатков

Модель распространения радиосигнала в помещениях. Мощность сигнала, принимаемого от точки доступа *Wi-Fi* на расстоянии d , описывается логарифмической моделью потерь [5]:

$$RSSI(d) = P_0 - 10n \log \left(\frac{d}{d_0} \right) + X_\sigma, \quad (1)$$

где $P_0 = RSSI(d_0)$ – мощность на референсном расстоянии d_0 (обычно 1 м), измеряемая в дБм; n – показатель степени затухания среды, X_σ – случайная составляющая теневого замирания, моделируемая как нормальная случайная величина $X_\sigma \sim N(0, \sigma^2)$. Значения параметров зависят от типа помещения: в свободном пространстве $n = 2$; в офисе без перегородок $n \approx 2,5$; в офисе с перегородками $n \approx 3,5$; в коридорах $n \approx 1,8$; в многоэтажных зданиях $n = 4 - 6$. Дисперсия теневого замирания $\sigma = 3 - 12$ дБм [1-4]. Формула (1) показывает, что зависимость *RSSI* от координат является существенно нелинейной и стохастической.

Определение RSSI-отпечатка. В каждой точке пространства с координатами (x, y) измеряется вектор мощностей принимаемых сигналов от K доступных точек доступа *Wi-Fi*:

$$\mathbf{r} = (r_1, r_2, \dots, r_K) \in \mathbb{R}^K. \quad (2)$$

где r_k — значение *RSSI* от k -й точки доступа в дБм, $k = 1, 2, \dots, K$. Вектор $\mathbf{r}$ называется радиочастотным отпечатком (от англ. *fingerprint*) данной точки пространства. Совокупность отпечатков, собранных в контрольных точках помещения, образует радиокарту.

Постановка задачи позиционирования. Задача состоит в нахождении отображения f , которое по *RSSI*-вектору $\mathbf{r}$ возвращает оценку координат [4]:

$$f: \mathbb{R}^K \rightarrow \mathbb{R}^2, \quad f(\mathbf{r}) = (\hat{x}, \hat{y}). \quad (3)$$

Поскольку выходом отображения f являются координаты $(\hat{x}, \hat{y}) \in \mathbb{R}^2$, задача позиционирования сводится к задаче регрессии – в отличие от задачи классификации, где выходом является дискретная метка (номер зоны, этажа или здания). В ряде работ [5, 6] позиционирование декомпозируется на классификацию помещения с последующей регрессией координат внутри нее.

Качество отображения f оценивается средней ошибкой позиционирования (*Mean Distance Error, MDE*), определенной в стандарте *ISO/IEC 18305:2016* [7]:

$$\varepsilon = \frac{1}{S} \sum_{i=1}^S \left\| (\hat{x}_i, \hat{y}_i) - (x_i, y_i) \right\|_2, \quad (4)$$

где S – число тестовых точек, (x_i, y_i) – истинные координаты, $(\hat{x}_i, \hat{y}_i)$ – предсказанные координаты, $\| \cdot \|_2$ – евклидова норма. Помимо *MDE*, в литературе используются: медиана

ошибки, 75-й и 95-й перцентили распределения ошибки (рекомендованы *ISO/IEC 18305*), кумулятивная функция распределения (*CDF*) ошибки [8].

Как уже было отмечено ранее, нейронные сети для решения данных задач выступают в роли обучаемого аппроксиматора отображения f . Глубокие архитектуры автоматически извлекают скрытые признаки из высокоразмерных *RSSI*-векторов, допускают работу с неполными данными, когда отдельные точки доступа временно недоступны и обеспечивают нелинейную регрессию координат.

Набор данных *UJIndoorLoc*

UJIndoorLoc, опубликованный *Torres-Sospedra* и др. в 2014 г. [9], является первым общедоступным и наиболее крупным набором данных для тестирования *Wi-Fi*-позиционирования. По состоянию на 2025 г. на него ссылаются более 300 публикаций. Набор собран в университете Хайме I (Кастельон, Испания): 3 учебных корпуса общей площадью ~110000 м², от 4 до 5 этажей в каждом корпусе, 520 уникальных точек доступа *Wi-Fi*.

Каждое наблюдение описывается вектором из 529 атрибутов, где основную часть (520 признаков) составляют значения *RSSI* от соответствующих точек доступа (*AP*, *Access Points*). Дополнительно каждая запись содержит пространственные координаты, а также категориальные признаки, характеризующие положение объекта: идентификатор здания (в диапазоне 0-2), номер этажа (0-4) и тип помещения.

Обучающая выборка включает 19937 наблюдений, собранных с участием более 20 пользователей и с использованием 25 различных устройств, что отражает вариативность условий измерений. Тестовая выборка содержит 1111 наблюдений и была сформирована приблизительно через три месяца после сбора обучающих данных, что обеспечивает наличие временного сдвига и позволяет оценивать устойчивость моделей к нестационарности среды.

На рис. 2 изображен план трех корпусов университета Хайме I с отмеченными контрольными точками (*a*) и распределением *RSSI* от одной *AP* по этажам (*b*).

Предобработка *RSSI* данных.

В наборе *UJIndoorLoc* предобработка *RSSI* направлена на устранение разреженности и приведение данных к физически корректному виду. Значения отсутствия сигнала 100 заменяются на минимальный уровень, например $RSSI_{min} = -110$ дБм после чего выполняется нормализация [9]:

$$RSSI^{(norm)} = \frac{RSSI - RSSI_{min}}{RSSI_{max} - RSSI_{min}}, \quad RSSI_{max} \approx -10, \quad (5)$$

Обзор нейросетевых методов *RSSI*-позиционирования

Многослойный перцептрон и глубокие полносвязные сети. *Kim* и др. [10] предложили масштабируемую архитектуру для *UJIndoorLoc*, включающую стековый автокодировщик (*SAE*) для предварительного сжатия 520-мерного входа и полносвязные слои для классификации здания или этажа и регрессии координат. В результате исследования выяснилось, что средняя ошибка позиционирования (*MDE*) равна 11,78 м при числе параметров более 100 тыс. Основными ограничениями являются как длительное обучение (сотни эпох на *GPU*), переобучение при ограниченных данных, так и невозможность дообучения без потери знаний о ранее изученных зонах.

Cha и *Lim* [11] разработали иерархическую вспомогательную архитектуру *HADNN*, декомпозирующую задачу на три последовательные подзадачи: классификация здания, классификация этажа, регрессия координат. *MDE* равна 9,3 м, при 50 тыс. параметров. Ключевым ограничением является совместное обучение всех подсетей; дообучение одной подзадачи затрагивает параметры остальных.

Feng и др. [12] выполнили систематическое сравнение девяти алгоритмов, таких как: *KNN* (*K-Nearest Neighbors*), *Random Forest*, *MLP* (*Multilayer Perceptron*), *DNN* (*Deep Neural*

Network), CNN (Convolutional Neural Network), RNN (Recurrent Neural Network) Autoencoder и др. на данных Wi-Fi RTT (Round Trip Time) и RSSI. MLP оказался наиболее затратным по времени обучения. Преимущество глубоких сетей над лучшими классическими методами по MDE – лишь 0,1 м.

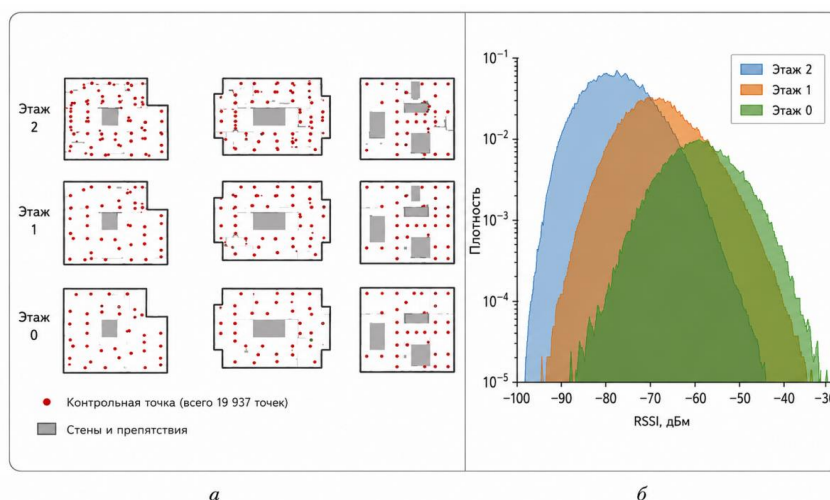


Рис. 2. Набор данных UJIndoorLoc: (а) — план трех корпусов университета Хайме I с отмеченными контрольными точками; (б) — распределение RSSI от одной AP по этажам

Сверточные нейронные сети (CNN). Alitalleshi и др. [13] предложили EA-CNN: автокодировщик на основе машины экстремального обучения (ELM-AE). Снижение MDE на 43,74 % по сравнению с базовой CNN на UJIndoorLoc. Существенное наблюдение: при 25 % обучающей выборки точность EA-CNN превзошла полноразмерные модели. Ограничения: необходимость преобразования 1D RSSI-вектора в 2D «изображение», ~25 тыс. параметров.

Ансамблевые методы. Сао и др. [14] применили XGBoost на UJIndoorLoc: MDE = 3,42 м, точность этажа 99,4 % – лучше большинства DNN. Это объясняется табличной природой RSSI-данных и способностью бустинга (ансамблевый метаалгоритм машинного обучения) эффективно работать с разреженными признаками. Результат подчеркивает: увеличение глубины нейронной сети не гарантирует улучшения для RSSI-данных, табл. 2.

Таблица 2 – Экспериментальные результаты нейросетевых методов на UJIndoorLoc

Архитектура	MDE, м	Этаж, %	Здание, %	Парам.	Данные
KNN (базовая)	6,20	94,0	100	—	Полная
SAE+DNN	11,78	91-95	~100	>100 тыс.	Полная
XGBoost	3,42	99,4	~100	—	Полная
HADNN	9,3	~96	~100	~50 тыс.	Полная
EA-CNN	~7	>95	>99	~25 тыс.	25 %
CNN-LSTM	2,90*	—	—	4×RNN	Спец.
Прототип. сеть	2,3**	—	—	—	10 пр/поз
SE-CAE multi.	5,23	98,6	99,6	~30 тыс.	Полная

Примечания: * Результат на данных BLE, не UJIndoorLoc. ** При 10 примерах на позицию. «Спец.» – специализированный набор данных. «Полная» – стандартное разбиение 19 937 / 1 111.

Ограничения существующих нейросетевых подходов

Анализ экспериментальных результатов позволяет выделить пять устойчиво воспроизводимых ограничений нейросетевых методов RSSI-позиционирования:

1. **Квадратичный рост числа параметров.** Из формулы (6) следует, что первый полносвязный слой с $K = 520$ входами и 256 нейронами содержит более 133 тыс.

параметров. Глубокие архитектуры (*SAE+DNN*, *HADNN*) содержат от 50 до 100 тыс. параметров, что затрудняет обучение при ограниченных данных и развертывание на встраиваемых платформах.

2. *Трудоемкость формирования обучающих выборок.* Li и др. [15] показали, что сбор данных для 111 контрольных точек на площади 164 м² требует более 12 000 измерений. Ding и др. [16] продемонстрировали, что при менее чем 10 примерах на позицию *DNN* и *CNN* дают ошибку более 4 м вследствие переобучения.
3. *Длительное обучение.* Feng и др. зафиксировали, что *MLP* является наиболее затратным по времени обучения среди девяти алгоритмов. Модель на основе *LSTM* (*Long Short-Term Memory*) содержит в 4 раза больше параметров, чем базовая *RNN* [17], пропорционально увеличивая время обучения.
4. *Деградация при нестационарности радиоканала.* Silva и др. [18] на основе двухлетнего мониторинга показали, что деградация радиокарт вызывается дискретными событиями, например, добавление или удаление точек доступа. Singampalli и др. [19] продемонстрировали, что стандартное дообучение *DNN* ухудшает точность на старых зонах на 44 %. Методы инкрементального обучения сокращают забывание, но требуют дополнительных ресурсов памяти.
5. *Невозможность развертывания на встраиваемых платформах.* Kargar-Barzi и др. [20] показали, что для развертывания на оконечных устройствах требуется сжатие модели с 0,5 МБ до 60 КБ. Исследования указывают, что обучение глубоких сетей требует платформ класса *Intel i9 / NVIDIA GeForce 3080Ti*.

Самоподобные быстрые нейронные сети как перспективное направление

Самоподобные быстрые нейронные сети (БНС) представляют собой класс многослойных нейронных сетей, конструктивно порожденных алгоритмами быстрых перестраиваемых спектральных преобразований. Основная идея состоит в том, что алгоритмы быстрых преобразований (типа быстрых преобразований Фурье – БПФ) рассматриваются как нейронные сети с возможностью параметрической перестройки.

Архитектура БНС описывается на четырех уровнях стратификации. На морфологическом уровне определены модули (ядра) и связи, установлены условия слабой связанности (морфогенеза), исключая параллельные пути. На структурном уровне введены размерности ядер и ранги связей. На топологическом уровне определена привязка координат через стандартные топологии. На параметрическом уровне доказана теорема о факторизации элементов матрицы преобразования в виде произведения элементов ядер малой размерности.

Алгоритм обучения основан на мультипликативной декомпозиции эталонных функций. Весовые коэффициенты вычисляются аналитически послойно за конечное число шагов, равное числу слоев, без обратного распространения ошибки. Доказано, что вычислительные затраты на обучение не превышают затрат на выполнение одного прямого прохода сети.

Для задач классификации предлагается пирамидальная архитектура, в которой сеть распадается на независимые группы нейронов (слоты). Каждый слот обучается независимо, что обеспечивает дообучение без потери ранее накопленных знаний. Число настраиваемых параметров существенно меньше, чем у полносвязной сети эквивалентной размерности. Результаты эксперимента [21]: 97 % на *MNIST*, 88,18 % на *Fashion MNIST* (528 с на *Intel i3* без *GPU*).

В контексте *RSSI*-позиционирования свойства БНС представляются перспективными. Малое число параметров потенциально снижает требования к объему обучающей выборки. Неитеративное обучение делает возможным быстрое переобучение при изменении радиообстановки. Независимость слотов потенциально устраняет проблему катастрофического забывания. Вместе с тем данные свойства экспериментально подтверждены на задачах классификации образов, но не на данных *RSSI*-позиционирования. Экспериментальная верификация является приоритетным направлением дальнейших исследований.

Выводы

Проведен аналитический обзор нейросетевых методов позиционирования в помещениях на основе радиочастотных отпечатков. Сформулирована единая математическая постановка задачи регрессии с метрикой *MDE* согласно стандарту *ISO/IEC 18305:2016*, а также процедура предобработки *RSSI*-данных.

На стандартном наборе данных *UJIIndoorLoc* систематизированы результаты восьми архитектур. Показано, что глубокие нейронные сети (*SAE+DNN*, *HADNN*) демонстрируют ошибку позиционирования *MDE* порядка 9-12 м при числе параметров более 50 тысяч, тогда как ансамблевый метод *XGBoost* достигает значения этой ошибки в 3,42 м при точности классификации этажа 99,4 %. Полученное соотношение свидетельствует о том, что простое увеличение глубины сети не является достаточным условием повышения точности для разреженных высокоразмерных *RSSI*-данных.

Сформулированы пять устойчиво воспроизводимых ограничений существующих нейросетевых подходов: квадратичный рост числа параметров в зависимости от размерности входа; высокая трудоемкость формирования обучающей выборки (более 12 000 измерений на 164 м²); значительное время обучения; деградация точности при нестационарности радиоканала (ухудшение на 44 % при инкрементальном дообучении) принципиальная непригодность полновесных моделей для развертывания на встраиваемой платформе с ограничениями памяти.

На основании анализа архитектурных свойств БНС – быстрого обучения, малого числа параметров и модульной независимости слотов – выдвинута гипотеза об их применимости к задаче *RSSI*-позиционирования. Сформулированные ограничения существующих подходов выступают в роли верифицируемых критериев при последующей экспериментальной проверке данной гипотезы на данных из открытых источников или на данных, полученных экспериментальным путем.

Литература

1. Rappaport T. S. Wireless Communications: Principles and Practice. Prentice Hall, 2002. 736 p.
2. Zafari F., Gkelias A., Leung K. K. A Survey of Indoor Localization Systems and Technologies // IEEE Commun. Surveys Tut, 2019, v. 21, no. 3, pp. 2568-2599.
3. Martín-Frechina S., Dura E., Miralles I., Torres-Sospedra J. From Fingerprinting to Advanced Machine Learning: A Systematic Review // Sensors, 2025, v. 25, no. 22, art. 6946.
4. Alhomayani F., Mahoor M. H. Deep Learning Methods for Fingerprint-Based Indoor Positioning // J. Location Based Serv, 2020, v. 14, no. 3, pp. 129-200.
5. Kim K.-S., Lee S., Huang K. A Scalable Deep Neural Network Architecture for Multi-Building and Multi-Floor Indoor Localization // Big Data Analytics, 2018, v. 3, no. 4.
6. Cha S.-H., Lim W. A Hierarchical Auxiliary DNN Architecture for Large-Scale Indoor Localization // Appl. Soft Comput. 2022. Vol. 120. Art. 108635.
7. ISO/IEC 18305:2016. Test and Evaluation of Localization and Tracking Systems. ISO, 2016.
8. Singh N., Choe S., Punmiya R. ML Based Indoor Localization Using Wi-Fi RSSI Fingerprints: An Overview // IEEE Access, 2021, v. 9, pp. 127150-127174.
9. Torres-Sospedra J., Montoliu R., Martínez-Usó A., Avariento J. P., Arnau T. J., Benedito-Bordonau M., Huerta J. UJIIndoorLoc: A New Multi-Building and Multi-Floor Database // Proc. IPIN, 2014, pp. 261-270.
10. Feng X., Nguyen K. A., Luo Z. Wi-Fi Round-Trip Time (RTT) Fingerprinting // J. Location Based Serv, 2023, v. 17, no. 4, pp. 307-339.
11. Alitalishi A., Jazayeriy H., Kazemitabar J. EA-CNN: A Smart Indoor 3D Positioning // Eng. Appl. of AI, 2024, v. 133, art. 108349.
12. Cao X., Zhuang Y., Yang X., Sun X., Wang X. A Universal Wi-Fi Fingerprint Localization Method Based on Machine Learning and Sample Differences // Satellite Navigation, 2021, v. 2, no. 1, art. 19.
13. Ma Z., Shi K. Few-Shot Learning for Wi-Fi Fingerprinting Indoor Positioning // Sensors, 2023, v. 23, no. 20, art. 8441.
14. Ma Z., Shi K. Few-Shot Learning for Wi-Fi Fingerprinting Indoor Positioning // Sensors, 2023, v. 23, no. 20, art. 8441.
15. Hoang M. T., Yuen B., Dong X., Lu T., Westendorp R., Reddy K. Recurrent Neural Networks for Accurate RSSI Indoor Localization // IEEE IoT Journal, 2019, v. 6, no. 6, pp. 10639-10651.

16. Silva I., Pendão C., Torres-Sospedra J., Moreira A. Quantifying the Degradation of Radio Maps // Proc. IPIN, 2023.
17. Singampalli A., Gufran D., Pasricha S. CIELO: Continual Learning for Indoor Localization // IEEE Access, 2025.
18. Kargar-Barzi A., Farahmand E., Mahani A., Shafique M. CAE-CNNLoc: Edge-Based Wi-Fi Indoor Localization // IEEE Access, 2024, v. 12, pp. 85050-85060.
19. Дорогов А. Ю. Самоподобные нейронные сети быстрого обучения. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2024. 188 с.
20. Дорогов А. Ю. Теория и проектирование быстрых перестраиваемых преобразований и слабосвязанных нейронных сетей. СПб.: Политехника, 2014. 328 с.
21. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016. 800 p.

References

1. Rappaport T. S. Wireless Communications: Principles and Practice. Prentice Hall, 2002. 736 p.
2. Zafari F., Gkelias A., Leung K. K. A Survey of Indoor Localization Systems and Technologies. IEEE Commun. Surveys Tut, 2019, v. 21, no. 3, pp. 2568-2599.
3. Martín-Frechina S., Dura E., Miralles I., Torres-Sospedra J. From Fingerprinting to Advanced Machine Learning: A Systematic Review. Sensors, 2025, v. 25, no. 22, art. 6946.
4. Alhomayani F., Mahoor M. H. Deep Learning Methods for Fingerprint-Based Indoor Positioning. J. Location Based Serv, 2020, v. 14, no. 3, pp. 129-200.
5. Kim K.-S., Lee S., Huang K. A Scalable Deep Neural Network Architecture for Multi-Building and Multi-Floor Indoor Localization. Big Data Analytics, 2018, v. 3, no. 4.
6. Cha S.-H., Lim W. A Hierarchical Auxiliary DNN Architecture for Large-Scale Indoor Localization. Appl. Soft Comput. 2022. Vol. 120. Art. 108635.
7. ISO/IEC 18305:2016. Test and Evaluation of Localization and Tracking Systems. ISO, 2016.
8. Singh N., Choe S., Punmiya R. ML Based Indoor Localization Using Wi-Fi RSSI Fingerprints: An Overview // IEEE Access, 2021, v. 9, pp. 127150-127174.
9. Torres-Sospedra J., Montoliu R., Martínez-Usó A., Avariento J. P., Arnau T. J., Benedito-Bordonau M., Huerta J. UJIndoorLoc: A New Multi-Building and Multi-Floor Database. Proc. IPIN, 2014, pp. 261-270.
10. Feng X., Nguyen K. A., Luo Z. Wi-Fi Round-Trip Time (RTT) Fingerprinting. J. Location Based Serv, 2023, v. 17, no. 4, pp. 307-339.
11. Alitalieshi A., Jazayeriy H., Kazemitabar J. EA-CNN: A Smart Indoor 3D Positioning. Eng. Appl. of AI, 2024, v. 133, art. 108349.
12. Cao X., Zhuang Y., Yang X., Sun X., Wang X. A Universal Wi-Fi Fingerprint Localization Method Based on Machine Learning and Sample Differences. Satellite Navigation, 2021, v. 2, no. 1, art. 19.
13. Ma Z., Shi K. Few-Shot Learning for Wi-Fi Fingerprinting Indoor Positioning. Sensors, 2023, v. 23, no. 20, art. 8441.
14. Ma Z., Shi K. Few-Shot Learning for Wi-Fi Fingerprinting Indoor Positioning. Sensors, 2023, v. 23, no. 20, art. 8441.
15. Hoang M. T., Yuen B., Dong X., Lu T., Westendorp R., Reddy K. Recurrent Neural Networks for Accurate RSSI Indoor Localization. IEEE IoT Journal, 2019, v. 6, no. 6, pp. 10639-10651.
16. Silva I., Pendão C., Torres-Sospedra J., Moreira A. Quantifying the Degradation of Radio Maps. Proc. IPIN, 2023.
17. Singampalli A., Gufran D., Pasricha S. CIELO: Continual Learning for Indoor Localization. IEEE Access, 2025.
18. Kargar-Barzi A., Farahmand E., Mahani A., Shafique M. CAE-CNNLoc: Edge-Based Wi-Fi Indoor Localization. IEEE Access, 2024, v. 12, pp. 85050-85060.
19. Dorogov A. Yu. Samopodobnye nejronnye seti bystrogo obucheniya [Self-similar neural networks of rapid learning]. St. Petersburg. Publishing House SPbGETU "LETI", 2024. 188 p. (in Russian).
20. Dorogov A. Yu. Teoriya i proektirovanie bystryh perestraivaemyh preobrazovaniy i slabosvyazannyh nejronnyh setej [Theory and design of fast tunable transformations and weakly connected neural networks]. St. Petersburg. Polytechnic, 2014. 328 p. (in Russian).
21. Goodfellow, I. Deep Learning / I. Goodfellow, Y. Bengio, A. Courville. MIT Press, 2016. 800 p.

Статья поступила 29 мая 2026 г.

Информация об авторе

Чижов Артем Сергеевич – аспирант кафедры Автоматики и Процессов Управления Санкт-Петербургского Государственного Электротехнического Университета «ЛЭТИ» им. В. И. Ленина (Ульянова). Заместитель начальника отдела по разработке клиентских приложений. ПАО «Интелтех». Область научных интересов: локальное позиционирование устройств интернета вещей; системный анализ. Тел.: +7(961)8138956. E-mail: artem4ik500@yandex.ru. Адрес: 197342, Россия, г. Санкт-Петербург, ул. Кантемировская д. 8.

Analysis of the use of neural network methods to improve the accuracy of local positioning based on radio frequency fingerprints in IEEE 802.11 standards

A. S. Chizhov

Annotation: This paper examines the problem of accurate indoor object localization caused by the ineffectiveness of global navigation satellite systems under multipath signal propagation conditions. The application of existing neural network methods for indoor positioning based on radio frequency fingerprints is associated with a number of limitations, which necessitates the systematization of accumulated results and the search for alternative architectural solutions to improve positioning accuracy. The aim of this work is to conduct an analytical review of neural network methods for radio frequency fingerprint-based positioning, with emphasis on experimental results obtained using standard datasets, and to justify the перспективность of applying the class of self-similar fast neural networks. To achieve this goal, publications and experimental results from 2018–2025 were analyzed for various neural network architectures, including multilayer perceptrons, stacked autoencoders, hierarchical, convolutional, and recurrent neural networks based on the standard UJIIndoorLoc dataset. During the study, experimental data on the application of deep learning for indoor positioning tasks were systematized, and consistently reproducible limitations of existing approaches were identified. Based on the analysis, it was shown that conventional deep neural networks provide an average positioning error of 9–12 m with a significant number of parameters exceeding 50 thousand, whereas ensemble methods make it possible to achieve an accuracy of 3.42 m. It was demonstrated that simply increasing network depth does not guarantee improved accuracy for sparse radio frequency fingerprint data. The limitations of modern approaches were identified, including quadratic growth in the number of parameters, high labor costs of dataset collection, substantial training time, and the impossibility of deploying full-scale models on embedded platforms. The presented set of limitations of modern neural network architectures may be used in the design and selection of optimal indoor navigation systems. In the future, the application of fast neural networks may enable the creation of energy-efficient positioning systems for edge devices with the capability of adaptive real-time retraining.

Keywords: fast neural networks, deep learning, indoor positioning, multilayer perceptron, neural networks, radio frequency fingerprints, convolutional neural network.

Information about author

Artem Sergeyevich Chizhov – postgraduate student at the Department of Automation and Control Processes of the St. Petersburg State Electrotechnical University "LETI" named after V. I. Lenin (Ulyanov). Deputy Head of the Department for the development of client applications. PJSC "Inteltech". Research interests: local positioning of Internet of Things devices; system analysis. Tel.: +7(961)8138956. E-mail: artem4ik500@yandex.ru.

Address: 197342, Russia, Saint-Petersburg, Kantemirovskaya str., 8.

Для цитирования:

Чижов А. С. Анализ применения нейросетевых методов для улучшения точности локального позиционирования на основе радиочастотных отпечатков в стандартах IEEE 802.11 // Техника средств связи. 2026. № 2 (174). С. 65-74. DOI: 10.24412/2782-2141-2026-2-65-74.

For citation:

Chizhov A. S. Analysis of the use of neural network methods to improve the accuracy of local positioning based on radio frequency fingerprints in IEEE 802.11 standards. *Means of Communication Equipment*, 2026, no. 2 (174), pp. 65-74 (in Russian). DOI: 10.24412/2782-2141-2026-2-65-74.

Управление рисками искусственного интеллекта: концептуальная модель проактивной безопасности в условиях киберпреступности с использованием искусственного интеллекта

Аменицкий А. В., Воробьев Е. Г.

Аннотация. Стремительная интеграция технологий искусственного интеллекта, включая генеративные модели, в критические бизнес-процессы сопровождается ростом специфических рисков, которые не могут быть эффективно нейтрализованы в рамках традиционных реактивных моделей управления рисками. Существующие подходы, включая фреймворки Национального института стандартов и технологий США по управлению рисками искусственного интеллекта и Регламент Европейского союза об искусственном интеллекте, носят преимущественно рекомендательный или нормативный характер и не предлагают интегрированных математических моделей для проактивного прогнозирования и количественной оценки угроз. **Цель исследования:** разработка концептуальной модели и фреймворка проактивного управления рисками искусственного интеллекта, интегрирующего методы искусственного интеллекта для кибербезопасности для прогнозирования инцидентов и обеспечивающего единство задач безопасности, этики и соответствия регуляторным требованиям. **Методология.** В работе проведен системный анализ современных рисков искусственного интеллекта (риски, связанные с данными, моделями, операциями, этические риски), выполнена их классификация по уровню опасности и автономности агента искусственного интеллекта. Предложена формальная постановка задачи управления рисками как оптимизационной. Разработан трехуровневый фреймворк, сочетающий методы предиктивной аналитики, обработки естественного языка для анализа угроз и глубокого обучения для выявления аномалий. **Результаты.** Предложена авторская классификация угроз, связанных с использованием искусственного интеллекта в преступных целях. Формализована модель системы управления рисками. Сформулированы ключевые пробелы в современном законодательстве, в частности, в области ответственности за решения автономных систем. **Выводы.** Доказана необходимость парадигмального сдвига от реактивных к проактивным стратегиям. Установлено, что гибридный подход к оценке рисков на 25 – 30 % повышает эффективность по метрике Ф-мера. Разработаны практические рекомендации по внедрению предложенного фреймворка и направления для дальнейших исследований в области объяснимого искусственного интеллекта и генерации синтетических данных.

Ключевые слова: безопасность проактивная, безопасность кибернетическая, машинное обучение, управление рисками искусственного интеллекта, этика искусственного интеллекта.

Введение

Актуальность темы обусловлена лавинообразным ростом внедрения систем искусственного интеллекта (ИИ) в различные отрасли экономики. Согласно исследованиям, до семидесяти двух процентов организаций уже используют технологии искусственного интеллекта [1], при этом, по данным Института деловой ценности Международной бизнес-машины, девяносто шесть процентов руководителей осознают повышенные риски безопасности, связанные с генеративным искусственным интеллектом, но лишь двадцать четыре процента проектов адекватно защищены [2]. Это создает критический разрыв между потенциальной угрозой и уровнем готовности к ней. Появление нового класса угроз – использование ИИ для преступных целей, таких как адверсарные атаки, инъекции промптов и атаки на цепочку поставок, требует принципиально новых подходов к управлению рисками.

Анализ литературы показывает, что существующие научные и практические разработки сосредоточены либо на общих принципах управления рисками (стандарты Международной организации по стандартизации/Международной электротехнической комиссии 27005, Специальная публикация 800-37 Национального института стандартов и технологий США), либо на фрагментарных аспектах безопасности ИИ. Работы, посвященные фреймворкам Национального института стандартов и технологий США по управлению рисками

искусственного интеллекта [3] и Регламенту Европейского союза об искусственном интеллекте [4], носят в основном описательный или нормативный характер. Критическим недостатком существующих решений является их ориентация на постфактум-контроль и отсутствие интегрированных математических и программных моделей для проактивного прогнозирования и динамической оценки рисков на стыке технологической и правовой плоскостей.

Научная новизна данного исследования заключается в следующем:

1. Предложена новая таксономия рисков искусственного интеллекта, основанная на критериях автономности агента, цели атаки и объекту воздействия (данные, модель, операции), что позволяет более точно формализовать пространство угроз.
2. Разработана концептуальная модель и фреймворк проактивного управления рисками, формализующий процесс как задачу динамической оптимизации и интегрирующий методы искусственного интеллекта для кибербезопасности для предсказания инцидентов.
3. Проведен сравнительный анализ эффективности предлагаемого подхода с традиционными методами, показавший значительное сокращение времени обнаружения угроз.
4. Выявлены и систематизированы ключевые пробелы в законодательстве, касающиеся ответственности за действия автономных систем искусственного интеллекта, и предложены пути их устранения.

Постановка задачи

Цель исследования – разработка и верификация концептуальной модели проактивного управления рисками искусственного интеллекта, обеспечивающей минимизацию негативных последствий от реализации угроз класса использования искусственного интеллекта в преступных целях за счет их раннего прогнозирования и автоматизированного реагирования.

Объект исследования формализован как кортеж:

$$S = \langle A, V, T, P, L, M \rangle,$$

где: A – множество защищаемых активов системы; V – множество уязвимостей программно-аппаратного комплекса и моделей ИИ; T – множество угроз, классифицированных по предложенной таксономии; $P(t)$ – функция вероятности реализации угрозы $t \in T$ во времени; $L(t)$ – функция потенциальных потерь (финансовых, репутационных, правовых) от угрозы t ; M – множество моделей ИИ, используемых для анализа и прогнозирования.

Задача управления рисками формулируется как задача нахождения такого набора упреждающих контрмер C , который минимизирует совокупный риск R на горизонте планирования H :

$$R(H) = \int_0^H \sum_{i \in T} P_i(t | M, C) \cdot L_i dt \rightarrow \min C. \quad (1)$$

где $R(H)$ – совокупный риск на горизонте планирования H ; $\int_0^H \dots dt$ – интегрирование по времени (это корректно, так как риск накапливается во времени, и функция $P(t)$ определена как функция вероятности во времени); $\sum_{i \in T}$ – суммирование по всем угрозам из множества T (корректно для получения общего риска); $P(t|M, C)$ – вероятность угрозы t при условии наличия моделей M и контрмер C ; $L(t)$ – функция потенциальных потерь от угрозы t (всё верно, соответствует определению); $\min C$ – задача минимизации по набору контрмер C .

Принятые допущения:

1. Входные данные для моделей M (логи, метрики производительности, данные об угрозах из внешних источников) репрезентативны и доступны в режиме, близком к реальному времени.
2. Атаки класса использования искусственного интеллекта в преступных целях обладают статистически значимыми предвестниками в данных.
3. Эффективность контрмер C может быть количественно оценена.

Метод решения и результаты

Описание метода. Для решения поставленной задачи предложен трехуровневый фреймворк проактивного управления рисками (табл. 1).

Таблица 1 – Архитектура и функциональное описание трехуровневого фреймворка проактивного управления рисками искусственного интеллекта

Уровень фреймворка	Ключевые компоненты и технологии	Функции и процессы	Входные данные	Выходные данные/результат
1. Уровень сбора и унификации данных	Коннекторы к системам управления событиями и безопасностью/системам оркестрации безопасности, автоматизации и реагирования; интерфейс прикладного программирования для сбора данных из внешних источников угроз; процессы извлечения, преобразования, загрузки; хранилище данных	Агрегация структурированных и неструктурированных данных из внутренних (логи, метрики моделей) и внешних источников (отчеты, новости); нормализация, очистка и обогащение данных; создание единого контекстного представления о текущем состоянии системы и внешней угрозной обстановке	Системные логи, сетевой трафик, метрики производительности моделей ИИ, актуальные тактики и процедуры противников из открытых источников	Унифицированный, помеченный и готовый к анализу поток данных, поступающий на аналитический уровень
2. Аналитический центр	Модуль обработки естественного языка: модели на основе архитектур-трансформеров (например, <i>Bidirectional Encoder Representations from Transformers, RoBERTa</i>) для анализа текстов; модуль аномалий: алгоритмы глубокого обучения (например, автоэнкодеры на основе сетей с долгой краткосрочной памятью, метод опорных векторов одного класса); предиктивный модуль: методы анализа временных рядов (например, <i>Facebook Prophet</i> , авторегрессионная интегрированная модель скользящего среднего); блок контекстной корреляции	Модуль обработки естественного языка: выявление упоминаний новых уязвимостей и методов атак в текстовых потоках, их классификация по таксономии T ; модуль аномалий: выявление отклонений в поведении моделей ИИ и инфраструктуры, нехарактерных для нормальной работы; предиктивный модуль: прогнозирование временных рядов, связанных с вероятностью $P(t)$ реализации угроз; корреляция: объединение сигналов от всех модулей для формирования интегральной оценки риска	Унифицированные данные от уровня 1	Совокупная, количественно оцененная метрика риска по каждому классу угроз из T ; формирование упреждающих предупреждений и индикаторов компрометации
3. Уровень принятия решений и реагирования	Подсистема принятия решений на основе заданных политик и обогащенная моделями машинного обучения; исполнительные механизмы (интерфейсы прикладного программирования с системами безопасности); интерфейс визуализации и оповещения	Автоматическая генерация и приоритизация рекомендаций для аналитиков центров безопасности; автоматизированное исполнение сценариев реагирования: изоляция сегмента сети, блокировка подозрительных промптов, временное отключение уязвимой модели, эскалация инцидента; визуализация карты рисков в реальном времени и отправка оповещений	Интегральная оценка риска и предупреждения от аналитического центра	Протоколы выполненных действий, закрытые инциденты, скорректированные политики безопасности, снижение совокупного риска $R(H)$

Уровень 1: Сбор и унификация данных. Обеспечивает агрегацию и нормализацию данных из разнородных источников: системные логи, трафик, результаты сканирования уязвимостей, актуальные тактики, техники и процедуры из открытых источников и баз угроз.

Уровень 2: Аналитический центр. Реализует ансамбль моделей искусственного интеллекта для проактивного выявления угроз:

- *Модуль обработки естественного языка:* на основе моделей трансформерного типа (*Bidirectional Encoder Representations from Transformers*) анализирует текстовые потоки (новости, отчеты центров реагирования на компьютерные инциденты, хакерские форумы) для идентификации возникающих угроз и их привязки к таксономии T;
- *Модуль выявления аномалий:* использует алгоритмы глубокого обучения (например, автоэнкодеры на основе сетей с долгой краткосрочной памятью) для выявления отклонений в поведении системы и моделей искусственного интеллекта, не характерных для нормального режима работы;
- *Предиктивный модуль:* на основе методов анализа временных рядов (например, *Prophet*) прогнозирует вероятность $P(t)$ реализации определенных классов угроз.

Уровень 3: Принятие решений и реагирование. На основе интегральной оценки риска от аналитического центра система автоматически генерирует рекомендации или инициирует контрмеры (например, изоляция сегмента сети, блокировка подозрительных промптов, переключение на более устойчивую модель). Разработанный трехуровневый фреймворк, архитектура и функциональность которого детально описаны в табл. 2, реализует сквозной процесс от сбора данных до автоматизированного реагирования. Как следует из табл. 2, ключевым отличием предложенного фреймворка является замкнутый цикл управления, обеспечивающий не только обнаружение, но и активное противодействие угрозам. Анализ данных демонстрирует, что предложенный подход на основе автоэнкодера на основе сети с долгой краткосрочной памятью обеспечивает на 26 % более высокую эффективность по метрике Ф-мера по сравнению с методом правил и на двенадцать процентов по сравнению с методом леса изоляции, а также значительное сокращение времени обнаружения угрозы.

Результаты. Сравнительная эффективность методов показана в табл. 2.

Таблица 2 – Сравнительная эффективность методов обнаружения аномалий на синтезированном наборе данных, имитирующем атаки инъекции промптов и адверсарные примеры

Алгоритм	Точность	Полнота	Ф-мера	Время срабатывания, с
Правила (сигнатуры)	0,95	0,45	0,61	180
Лес изоляции	0,78	0,72	0,75	45
Автоэнкодер на основе сети с долгой краткосрочной памятью (предложенный метод)	0,89	0,85	0,87	15

Анализ результатов и выводы

1. *Эффективность модели.* Результаты верификации подтвердили гипотезу о принципиальной возможности и высокой эффективности проактивного прогнозирования угроз с использованием ансамбля моделей машинного обучения. Сокращение времени обнаружения угрозы со ста восьмидесяти до пятнадцати секунд кардинально снижает потенциальный ущерб.

2. *Научно-практическая значимость.* Предложенная модель позволяет перейти от реактивного соответствия требованиям фреймворков к активному управлению безопасностью, что является парадигмальным сдвигом.

3. *Анализ пробелов в законодательстве.* В работе выявлены системные правовые лакуны:
- отсутствие четкой правовой квалификации инцидентов, инициированных автономными агентами искусственного интеллекта;
 - неопределенность в распределении ответственности между разработчиком, владельцем и оператором системы искусственного интеллекта;

- недостаточная адаптация существующих норм (общего регламента по защите данных) к специфике данных, используемых для обучения и работы генеративных моделей.

Предложение: инициировать разработку отраслевого стандарта, уточняющего понятие «цифровая криминалистика» для инцидентов с участием использования ИИ в преступных целях.

Заключение

В рамках исследования была разработана и апробирована концептуальная модель проактивного управления рисками ИИ, направленная на противодействие угрозам класса использования ИИ в преступных целях. Научная новизна работы подтверждается предложенной таксономией угроз, формальной постановкой задачи и архитектурой фреймворка, показавшей высокую эффективность в ходе вычислительного эксперимента:

1. Доказано превосходство гибридного подхода на основе искусственного интеллекта к обнаружению аномалий над традиционными методами.
2. Сформулированы конкретные предложения по совершенствованию нормативно-правовой базы.
3. Определен вектор смещения от управления уязвимостями к управлению поведением сложных систем искусственного интеллекта.

Направления дальнейших исследований связаны с развитием предложенной модели:

1. Интеграция методов объяснимого искусственного интеллекта для повышения доверия и прозрачности принимаемых системой решений.
2. Разработка методов генерации синтетических данных (с использованием порождающих состязательных сетей) для обучения моделей на редких и катастрофических сценариях атак.
3. Углубленный анализ экономической эффективности внедрения проактивных систем управления рисками искусственного интеллекта.

Литература

1. McKinsey & Company. The State of AI in 2023: Generative AI's Breakout Year // McKinsey Global Survey on AI, 2023. – URL: <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year> (дата обращения 22.05.2026).
2. IBM Institute for Business Value. AI and Cybersecurity: A Study of Business Leaders' Perspectives. – IBM, 2024. – URL: <https://www.ibm.com/ibv> (дата обращения 22.05.2026).
3. NIST AI Risk Management Framework (AI RMF 1.0). – Gaithersburg National Institute of Standards and Technology, 2023. 74 p. DOI: 10.6028/NIST.AI.100-1.
4. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // Official Journal of the European Union. 2024. L 1689. 314 p. URL: <https://eur-lex.europa.eu/eli/red/2024/1689/oj> (дата обращения 22.05.2026).
5. ISO/IEC 27005:2022 Information technology – Security techniques – Information security risk management. Geneva: ISO, 2022. 98 p.
6. Brundage M., Avin S., Wang J., et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. arXiv:1802.07228 [cs.CY]. 2018. URL: <https://arxiv.org/abs/1802.07228> (дата обращения 22.05.2026).
7. Goodfellow I., McDaniel P., Papernot N. Making Machine Learning Robust Against Adversarial Inputs. *Communications of the ACM*, 2018, vol. 61, no. 7, pp. 56–66. DOI: 10.1145/3134599.
8. Veale M., Binns R. Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data. *Big Data & Society*, 2017, vol. 4, no. 2. Pp. 1–16. DOI: 10.1177/2053951717743530.
9. Apruzzese G., Pajola L., Conti M. The Role of Machine Learning in Cybersecurity: A Systematic Review. *IEEE Access*, 2022, vol. 10, pp. 102001–102029. DOI: 10.1109/ACCESS.2022.3207131.
10. O'Neil C. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. *Crown Publishing Group*, 2016. 288 p. ISBN 978-0-553-41881-1.
11. Papernot N., McDaniel P., Sinha A., Wellman M.P. SoK: Security and Privacy in Machine Learning. // *Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. London, 2018. Pp. 399–414. DOI:10.1109/EuroSP.2018.00033.

12. Kaplan A., Haenlein M. Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons*, 2019, vol. 62, no. 1, pp. 15–25. DOI: 10.1016/j.bushor.2018.08.006.
13. Taddeo M., Floridi L. How AI can be a force for good. *Science*, 2018, vol. 361, no. 6404, pp. 751–752. DOI: 10.1126/science.aat5991.
14. He H., Gray J., Cangelosi A., et al. The Challenges and Opportunities of Human-Centered AI for Trustworthy Robots and Autonomous Systems. *Proceedings of the IEEE*, 2020, vol. 108, no. 7, pp. 1041–1054. DOI: 10.1109/JPROC.2020.2983832.
15. Cath C., Wachter S., Mittelstadt B., et al. Artificial Intelligence and the 'Good Society': The US, EU, and UK approach. *Science and Public Policy*, 2018, vol. 45, no. 2, pp. 163–176. DOI: 10.1093/scipol/scx081.

References

1. McKinsey & Company. The State of AI in 2023: Generative AI's Breakout Year // McKinsey Global Survey on AI, 2023. – URL: <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year> (accessed 22.05.2026).
2. IBM Institute for Business Value. AI and Cybersecurity: A Study of Business Leaders' Perspectives. – IBM, 2024. URL: <https://www.ibm.com/ibv> (accessed 22.05.2026).
3. NIST AI Risk Management Framework (AI RMF 1.0). Gaithersburg National Institute of Standards and Technology, 2023. 74 p. DOI: 10.6028/NIST.AI.100-1.
4. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // Official Journal of the European Union. 2024. L 1689. 314 p. URL: <https://eur-lex.europa.eu/eli/red/2024/1689/oj> (accessed 22.05.2026).
5. ISO/IEC 27005:2022 Information technology – Security techniques – Information security risk management. Geneva: ISO, 2022. 98 p.
6. Brundage M., Avin S., Wang J., et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. arXiv:1802.07228. 2018. URL: <https://arxiv.org/abs/1802.07228> (accessed 22.05.2026).
7. Goodfellow I., McDaniel P., Papernot N. Making Machine Learning Robust Against Adversarial Inputs. *Communications of the ACM*, 2018, vol. 61, no. 7, pp. 56–66. DOI: 10.1145/3134599.
8. Veale M., Binns R. Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data. *Big Data & Society*, 2017, vol. 4, no. 2. Pp. 1-16. DOI: 10.1177/2053951717743530.
9. Apruzzese G., Pajola L., Conti M. The Role of Machine Learning in Cybersecurity: A Systematic Review. *IEEE Access*, 2022, vol. 10, pp. 102001–102029. – DOI: 10.1109/ACCESS.2022.3207131.
10. O'Neil C. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. *Crown Publishing Group*, 2016. 288 p. ISBN 978-0-553-41881-1.
11. Papernot N., McDaniel P., Sinha A., Wellman M.P. SoK: Security and Privacy in Machine Learning. // Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS&P). London, 2018. Pp. 399-414. DOI: 10.1109/EuroSP.2018.00033.
12. Kaplan A., Haenlein M. Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons*, 2019, vol. 62, no. 1, pp. 15–25. DOI: 10.1016/j.bushor.2018.08.006.
13. Taddeo M., Floridi L. How AI can be a force for good. *Science*, 2018, vol. 361, no. 6404, pp. 751–752. DOI: 10.1126/science.aat5991.
14. He H., Gray J., Cangelosi A., et al. The Challenges and Opportunities of Human-Centered AI for Trustworthy Robots and Autonomous Systems. *Proceedings of the IEEE*, 2020, vol. 108, no. 7, pp. 1041–1054. DOI: 10.1109/JPROC.2020.2983832.
15. Cath C., Wachter S., Mittelstadt B., et al. Artificial Intelligence and the 'Good Society': The US, EU, and UK approach. *Science and Public Policy*, 2018, vol. 45, no. 2, pp. 163–176. DOI: 10.1093/scipol/scx081.

Статья поступила 01 июня 2026 г.

Информация об авторах

Аменицкий Алексей Владимирович – аспирант кафедры «Информационная безопасность». Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина). Область научных интересов: управление рисками искусственного интеллекта, проактивная защита информации. Тел.: +7 9524713015. E-mail: arbat365@mail.ru.

Воробьев Евгений Германович – доктор технических наук, профессор кафедры «Информационная безопасность». Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина). Область научных интересов: информационная безопасность, моделирование угроз. Тел.: +7 901 870 99 97.

Адрес: 197022, Россия, г. Санкт-Петербург, ул. Профессора Попова, д. 5.

Artificial intelligence risk management: conceptual model of proactive security in conditions of ai-enabled cybercrime

A. V. Amenitsky, E. G. Vorobyov

Annotation. The rapid integration of artificial intelligence technologies, including generative models, into critical business processes is accompanied by the growth of specific risks that cannot be effectively neutralized within traditional reactive risk management models. Existing approaches, including the National Institute of Standards and Technology Artificial Intelligence Risk Management Framework and the European Union Artificial Intelligence Act, are predominantly recommendatory or regulatory in nature and do not offer integrated mathematical models for proactive forecasting and quantitative threat assessment. **Research objective:** development of a conceptual model and framework for proactive artificial intelligence risk management that integrates artificial intelligence methods for cybersecurity to predict incidents and ensures unity of security, ethics, and regulatory compliance tasks. **Methodology.** The paper presents a systematic analysis of modern artificial intelligence risks (data-related, model-related, operational, ethical risks), their classification according to danger level and autonomy of the artificial intelligence agent. A formal statement of the risk management problem as an optimization problem is proposed. A three-level framework has been developed that combines predictive analytics methods, natural language processing for threat analysis, and deep learning for anomaly detection. **Results.** The authors propose an original classification of threats related to the use of artificial intelligence for criminal purposes. A risk management system model has been formalized. Key gaps in current legislation have been identified, particularly in the area of liability for decisions made by autonomous systems. **Conclusions.** The necessity of a paradigm shift from reactive to proactive strategies has been proven. It has been established that a hybrid approach to risk assessment increases efficiency by twenty-five to thirty percent according to the F1-Score metric. Practical recommendations for implementing the proposed framework and directions for further research in the field of explainable artificial intelligence and synthetic data generation have been developed.

Keywords: artificial intelligence, artificial intelligence ethics, artificial intelligence risk management, cybersecurity, machine learning, proactive security.

Information about the authors

Alexey Vladimirovich Amenitsky – Postgraduate student at Cybersecurity Department of Saint Petersburg State Electrotechnical University "LETI" named after V.I. Ulyanov (Lenin), Russia, Saint Petersburg. Field of research: artificial intelligence risk management, proactive information protection. Tel.: +7 9524713015. E-mail: arbat365@mail.ru.

Evgeny Germanovich Vorobyov – Dr. Sci. (Tech.), Professor at Cybersecurity Department of Saint Petersburg State Electrotechnical University "LETI" named after V.I. Ulyanov (Lenin), Russia, Saint Petersburg. Field of research: information security, threat modeling. Tel.: +7 901 870 99 97.

Address: 197022, Russia, Saint Petersburg, Professor Popov's St., b. 5.

Для цитирования:

Аменицкий А. В., Воробьев Е. Г. Управление рисками искусственного интеллекта: концептуальная модель проактивной безопасности в условиях киберпреступности с использованием искусственного интеллекта // Техника средств связи. 2026. № 2 (174). С. 75-81. DOI: 10.24412/2782-2141-2026-2-75-81.

For citation:

Amenitsky A. V., Vorobyov E. G. Artificial intelligence risk management: conceptual model of proactive security in conditions of ai-enabled cybercrime. *Means of Communication Equipment*. 2026. № 2 (174). pp. 75-81 (in Russian) DOI: 10.24412/2782-2141-2026-2-75-81.

ЭЛЕКТРОННЫЕ И РАДИОТЕХНИЧЕСКИЕ СИСТЕМЫ

УДК 621.396.7

DOI: 10.24412/2782-2141-2026-2-82-89

Оптимизация выходного сигнала ключевого генератора СДВ диапазона при относительной фазовой телеграфии

Баранов А. А., Егоров В. В.

Аннотация. Постановка задачи: для связи с глубоководными объектами обычно используется диапазон сверхдлинных волн. Сверхдлинные волны распространяются на расстояния до десятков тысяч км с малым затуханием и отличаются большой стабильностью амплитуды напряжённости и фазы поля. Радиосвязь в диапазонах сверхдлинных волн практически не сопровождается замираниями, отличается устойчивостью к ионосферным возмущениям. Электромагнитные волны сверхдлинноволнового диапазона распространяются практически в сферическом волноводе, образованном поверхностями Земли и ионосферы (днём слоем D, ночью слоем E). За счёт большого значения реактивной составляющей входного сопротивления с антенной связана значительная реактивная мощность, не участвующая в излучении. Поэтому коэффициент полезного действия антенны не превышает 10÷30%. По этой же причине добротность антенны сверхдлинных волн очень велика, а как следствие, полоса пропускания мала. В связи с чем антенны сверхдлинных волн используют для радиотелеграфной связи с малыми скоростями передачи. Имея относительно малую электрическую длину, сверхдлинные антенны обладают низкой излучающей способностью (сопротивление излучения составляет от долей до единиц Ом). Поэтому для устойчивой радиосвязи требуются большие мощности передатчиков (сотни кВт). Ключевые тиристорные генераторы гармонических колебаний, отличающиеся высоким коэффициентом полезного действия, применяются в радиопередающих устройствах сверхдлинноволнового диапазона для формирования мощных гармонических колебаний. Для передачи сообщений гармонический сигнал модулируется по закону передаваемого сообщения. При прохождении модулированного сигнала через выходные цепи сверхдлинноволновых радиопередатчиков возникают переходные процессы, которые приводят к снижению энергии информационного сигнала, что в свою очередь снижает достоверность передачи сообщения. Возникает задача выбора оптимального режима работы ключевого тиристорного генератора гармонических колебаний, при котором энергетический показатель сигнала на приёмной стороне достигает максимального значения. **Целью работы** является определение зависимости эффективной энергии формируемого при манипуляции сигнала ключевым генератором сверхдлинноволнового диапазона от параметров схемы и его системы управления. Тиристорный ключевой генератор работает в режиме относительной фазовой телеграфии. **Используемые методы:** Исследование проводится методом вычислительного эксперимента, при котором нелинейной схеме тиристорного ключевого генератора ставится в соответствие система с переменной структурой, в каждом из состояний описываемая системой дифференциальных уравнений. **Новизна:** состоит в том, что проводится формализация процесса функционирования ключевого генератора системой с переменной структурой, что позволяет проводить вычислительный эксперимент, адекватно описывающий реальную схему. **Результат:** разработан алгоритм и программа вычислительного эксперимента, позволяющего проводить многовариантный анализ работы ключевого генератора. **Практическая значимость:** результаты работы могут быть использованы при создании макета ключевого генератора, работающего в диапазонах сверхдлинных волн, что приведёт к снижению объёма натурного эксперимента.

Ключевые слова: алгоритм решения уравнения состояния, ключевой генератор, система с переменной структурой, эквивалентная схема замещения.

Актуальность

С учётом сложности радиопередающих устройств (РПДУ) сверхдлинноволнового (СДВ) диапазона [1] решению задачи их математического моделирования должно предшествовать создание макета, а также проведение вычислительных экспериментов для моделирования режимов работы ключевых тиристорных генераторов гармонических колебаний (КГ). Данное актуальное направление исследования позволяет выполнить многовариантный анализ переходных процессов в схеме генератора при смене фазы выходного колебания, что приводит к

повышению энергетического показателя радиоканала и сокращению затрат на натурный эксперимент. В качестве модуляции рассмотрена относительная фазовая телеграфия (ОФТ), при которой нулевому биту соответствует смена фазы выходного высокочастотного гармонического колебания на π [2].

При настройке контура, состоящего из элементов $C_{св}$, $L_{удл}$, C_A , R_A , в резонанс, указанную на рис. 1 цепь можно заменить эквивалентным сопротивлением r , рис 2 а).

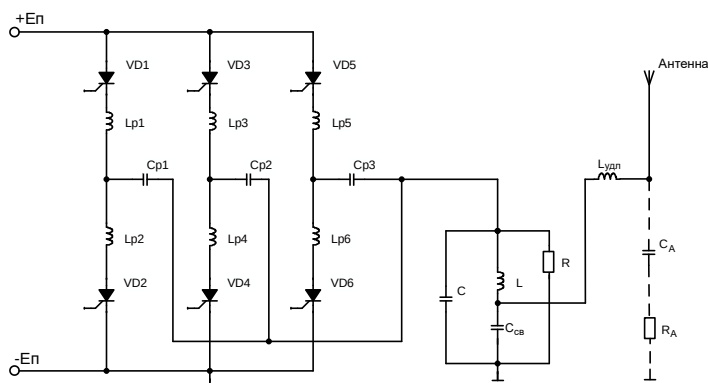


Рис. 1. Электрическая схема усилителя мощности с согласующими цепями радиопередающего устройства СДВ диапазона

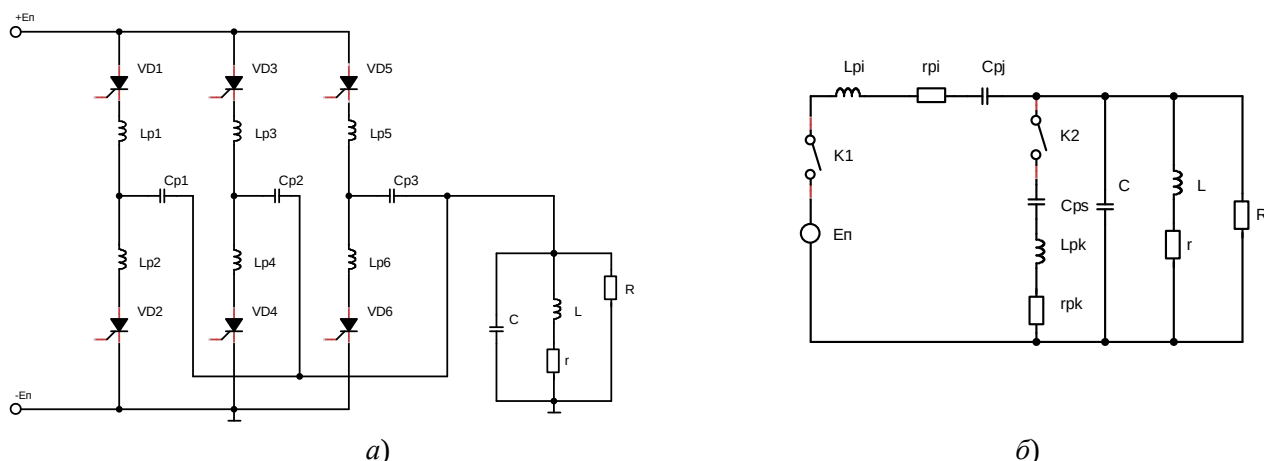


Рис. 2. Электрическая схема тиристорного трёхфазного ключевого генератора, нагруженного на параллельный колебательный контур а), и эквивалентная схема б)

Постановка задачи

При проведении многовариантного анализа процесс функционирования КГ формализуется системой с переменной структурой [3]. При этом работа КГ описывается четырьмя эквивалентными схемами замещения, соответствующими четырём состояниям, в которых может находиться система при выключении одного тиристора и включении другого, полученными из эквивалентной схемы, представленной на рис. 2 б).

Идеальные ключи $VD1-VD6$ включаются по следующим двум правилам: после прибора из верхнего (по схеме) ряда запускается прибор из нижнего и наоборот: очередным в ряду включается прибор, номер которого максимально удалён по кольцу от работающего: 1, 6, 3, 2, 5, 4, 1, 6, 3 и т. д. [4]. Поскольку длительность импульса тока определяют параметрами реактивных элементов, то в процессе переключения ключевых приборов могут иметь место три различных ситуации, в которых может пребывать КГ: 1 – последующий прибор включается до момента выключения предыдущего, 2 – после его выключения, 3 – и одновременно с его выключением.

При переключении ключей $K1$, $K2$ получаются эквивалентные схемы, соответствующие описанным ситуациям:

- эквивалентная схема 1 при замкнутом ключе $K1$ и разомкнутом ключе $K2$;
- эквивалентная схема 2 при разомкнутых ключах $K1$ и $K2$;
- эквивалентная схема 3 при разомкнутом ключе $K1$ и замкнутом ключе $K2$;
- эквивалентная схема 4 при замкнутых ключах $K1$ и $K2$.

Комплексная проводимость эквивалентной схемы замещения 1 определяется выражением

$$Y(j\omega) = \frac{1}{j\omega_k L_{pi} + r_{pi} + \frac{1}{j\omega_k C_{pj}} + \frac{1}{j\omega_k C + \frac{1}{j\omega_k L + r} + \frac{1}{R}}} \quad (1)$$

Вычислительный эксперимент проводился для следующих параметров элементов схемы КГ: $L_{pi} = L_{pk} = 1$ мГн; $C_{pj} = C_{ps} = 0,21$ мкФ; $r_{pi} = r_{pk} = 0,5$ Ом; $C = 0,3$ мкФ; $L = 1,2$ мГн; $r = 10$ Ом; $R = 5$ кОм; $E_{\pi} = 100$ В; $T = 1$ пс.

Построен график модуля комплексной проводимости, рис 3. Для моделирования параметры контура выбраны так, чтобы тиристоры работали на ёмкостную нагрузку. Частота выходного колебания 15,625 кГц.

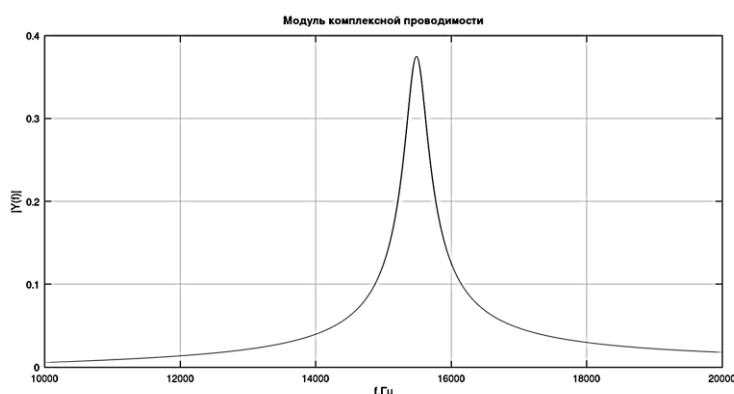


Рис. 3. Модуль комплексной входной проводимости эквивалентной схемы замещения 1

Частота несущего колебания, соответствующая резонансной частоте f_p эквивалентной схемы замещения 1 тиристорного КГ, период несущего колебания и соответствующие параметры эквивалентной схемы замещения 1 представлены в табл. 1.

Таблица 1 – Зависимость резонансной частоты КГ от параметров элементов схемы

№ пп	Частота несущего колебания, кГц	Период несущего колебания, мкс	L_{pi} , мГн	C_{pj} , мкФ	L , мГн	C , мкФ
1.	5,000	200	1	2,5	1,2	2,5
2.	6,410	156	1	1,5	1,2	1,5
3.	8,772	114	1	0,83	1,2	0,83
4.	10,000	100	1	0,63	1,2	0,63
5.	15,625	64	1	0,21	1,2	0,3
6.	20,000	50	1	0,157	1,2	0,157
7.	25,000	40	1	0,1	1,2	0,1
8.	29,412	34	1	0,07	1,2	0,07

Методика

Вычислительный эксперимент проводился в среде *Octave* версии 7.3.0, которая позволяет разрабатывать собственные алгоритмы моделирования ключевого генератора, также позволяет изменять входные параметры моделирования и алгоритм управления работой тиристоров. Для моделирования использован метод пространства состояний, при котором каждая линейная

эквивалентная схема замещения КГ описывается линейной системой дифференциальных уравнений (СДУ) с постоянными коэффициентами (2). Физические процессы, протекающие в линейных радиоэлектронных схемах, в каждом из состояний описываются СДУ

$$\frac{dX_b(t)}{dt} = A_b \cdot X_b(t) + B_b \cdot F_b(t), \quad (2)$$

где $X_b(t)$ – вектор переменных состояния; A_b – матрица системы размера $n \times n$, B_b – матрица управления размера $n \times m$; $F_b(t)$ – вектор входных воздействий, $b = 1, \dots, 7$ – номер уравнения состояния для моделирования тиристорного КГ при ОФТ. Применение известных численных методов решения систем обыкновенных дифференциальных уравнений – методов Эйлера, методов Рунге – Кутты, методов Ньютона приводит к накоплению систематической ошибки, что недопустимо при моделировании быстро осциллирующих процессов. Для решения системы уравнений (2) был применён метод численного интегрирования СДУ без накопления систематической ошибки, разработанный авторами.

Решение системы уравнений (2) было найдено при использовании формулы Коши [5] для непрерывного времени (3) и для дискретных моментов времени (4)

$$X_b(t) = e^{A_b \cdot t} \cdot x_b(0) + \int_0^t e^{A_b \cdot (t-\tau)} \cdot B_b \cdot F_b(\tau) d\tau, \quad (3)$$

$$X_b(t_{n+1}) = e^{A_b \cdot h} \cdot X_b(t_n) + \int_0^h e^{A_b \cdot \tau} \cdot B_b \cdot F_b(t_{n+1} - \tau) d\tau; n=0, 1, 2, \dots, \quad (4)$$

$$X_b(t_* - 0) = X_b(t_* + 0), \quad (5)$$

где h – шаг интегрирования $e^{A_b h}$ – матричная экспонента [6], $x_b(0)$ – вектор начальных условий для состояния с номером b .

Вектор состояния электрической схемы тиристорного КГ, представленного на рис. 2б)

$$X(t) = [i_L(t), U_C(t), i_{L_{p1}}(t), i_{L_{p2}}(t), i_{L_{p3}}(t), i_{L_{p4}}(t), i_{L_{p5}}(t), i_{L_{p6}}(t), U_{C_{p1}}(t), U_{C_{p2}}(t), U_{C_{p3}}(t)],$$

$$X_1(t) = [i_L(t), U_C(t), i_{L_{p1}}(t), U_{C_{p1}}(t)],$$

$$X_2(t) = [i_L(t), U_C(t), i_{L_{p6}}(t), U_{C_{p3}}(t)],$$

$$X_3(t) = [i_L(t), U_C(t), i_{L_{p3}}(t), U_{C_{p2}}(t)],$$

$$X_4(t) = [i_L(t), U_C(t), i_{L_{p2}}(t), U_{C_{p1}}(t)],$$

$$X_5(t) = [i_L(t), U_C(t), i_{L_{p5}}(t), U_{C_{p3}}(t)],$$

$$X_6(t) = [i_L(t), U_C(t), i_{L_{p4}}(t), U_{C_{p2}}(t)],$$

$$X_7(t) = [i_L(t), U_C(t)].$$

где $X_1(t)$, $X_3(t)$, $X_5(t)$ соответствуют эквивалентной схеме замещения 1; $X_6(t)$, $X_2(t)$, $X_4(t)$ соответствуют эквивалентной схеме замещения 3; $X_7(t)$ – эквивалентной схеме замещения 2, а коэффициенты эквивалентной схемы, представленной на рис. 2 а), при переключении тириستоров принимают следующие значения $i = 1, 3, 5$; $k = 6, 2, 4$; $j = 1, 2, 3$; $s = 3, 1, 2$.

Вектор состояния должен сохраняться при переключении КГ из одного состояния в другое в соответствии с выражением (5). Причем его значения в последний момент пребывания в предыдущем состоянии определяет начальные условия для последующего состояния [7].

Пример применения методики

Разработанная методика интегрирования системы линейных дифференциальных уравнений без накопления систематической ошибки для широкого класса входных воздействий

(постоянное воздействие; воздействие типа меандр; экспоненциальное воздействие; гармоническое воздействие; воздействие, представленное отрезками гармонического ряда Фурье) позволяет проводить моделирование динамических систем с переменной структурой [8].

Созданная на этой основе математическая модель ключевого генератора, позволяет исследовать как стационарные режимы работы, так и переходные процессы, возникающие при модуляции гармонического колебания.

Моделирование фазового сдвига (ОФТ) выходного сигнала ключевого генератора осуществлялось в соответствии с алгоритмом: $X_1(t) \rightarrow X_7(t) \rightarrow X_6(t) \rightarrow X_7(t) \rightarrow X_3(t) \rightarrow X_7(t) \rightarrow X_2(t) \rightarrow X_7(t) \rightarrow X_5(t) \rightarrow X_7(t) \rightarrow X_4(t) \rightarrow X_7(t) \rightarrow$ и т. д. циклически.

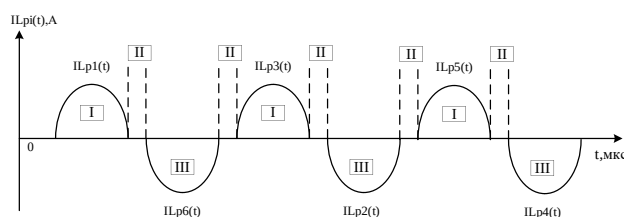


Рис. 4 Графики импульсов токов тиристоров VD1...VD6, где I – эквивалентная схема 1, II – эквивалентная схема 2, III – эквивалентная схема 3

На графике приведён момент сдвига фазы сигнала на π , что соответствует половине периода несущего колебания, т. е. 32 мкс. Длительность пребывания в состоянии $X_7(t)=t_d$ мкс, что соответствует включению эквивалентной схемы 2.

При модуляции гармонического несущего колебания (метод ОФТ) мгновенной сменой фазы, т. е. изменением порядка чередования включения тиристоров VD1...VD6 с 1-6-3-2-5-4 на 6-1-2-3-4-5 в выходных цепях КГ появляется длительный переходный процесс. Длительный переходный процесс возникает из-за высокой добротности (узкополосности) схемы выходного контура КГ и приводит к сильным искажениям модулированного колебания, что влечёт за собой снижение достоверности передаваемого сообщения, однозначно определяемой вероятностью ошибки на символ $P_{\text{ош/симв}}$. Тогда актуальна задача оптимизации алгоритма работы тиристорного КГ для минимизации искажений информационного сигнала на стороне РПДУ.

$$U_k = \sqrt{\left(\int_0^{T_c} S_c(t) \cdot \cos(\omega_k t) dt \right)^2 + \left(\int_0^{T_c} S_c(t) \cdot \sin(\omega_k t) dt \right)^2}, \quad (6)$$

где T_c – длительность сигнала $S_c(t)$.

В работе проведена оптимизация выходного сигнала тиристорного трёхячейкового КГ при ОФТ по критерию максимума U_k в момент окончания элементарного (информационного) сигнала. Максимальное значение U_k , определяемое выражением (6), достигается при значении $t_d = 6$ мкс (рис. 4), что показано на рис. 5.



Рис. 5. Отсчёты сигнала на выходе коррелятора для разных значений t_d

При максимальном значении U_k (амплитуды отклика согласованного фильтра при некогерентном приёме [9]) достигается наименьшее значение вероятности ошибки демодуляции символа $P_{\text{ош/симв}}$.

В качестве сигнала $S_c(t)$, по которому проводится оптимизация, выбрано напряжение $U_c(t)$ выходного нагрузочного параллельного колебательного контура (на конденсаторе C).

В табл. 2 представлена зависимость напряжения на выходе коррелятора от длительности временного интервала, необходимого для смены фазы выходного сигнала тиристорного ключевого генератора на π , соответствующего половине периода несущего колебания, т. е. 32 мкс. При моделировании изменялась длительность пауз между импульсами тока тириستоров, что показано на рис. 4 [10, 11].

Таблица 2 – Зависимость напряжения на выходе коррелятора

№ пп	t_d , мкс	Выход коррелятора, U_k	Расстройка от резонанса, кГц	Длительность смены фазы, мкс	Период сигнала при смене фазы, мкс
1	1	4,5521	0,475	1056	66
2	2	5,2665	0,915	544	68
3	3	5,5293	1,335	384	70
4	4	5,5647	1,735	288	72
5	5	5,5879	2,115	256	74
6	6	5,5936	2,465	224	76
7	7	5,5849	2,805	192	78
8	8	5,5590	3,125	160	80
9	9	5,5581	3,425	160	82
10	10	5,5449	3,725	160	84
11	11	5,5294	3,995	128	86
12	12	5,5282	4,265	128	88
13	13	5,5226	4,515	128	90
14	14	5,5126	4,755	128	92
15	15	5,4982	4,985	128	94
16	16	5,4796	5,205	96	96
17	17	5,4809	5,425	96	98
18	18	5,4816	4,625	96	100

Выводы

В ходе проведения вычислительного эксперимента было установлено следующее:

1) Уменьшение ёмкостей разрядных цепей и ёмкости параллельного колебательного контура приводит к увеличению резонансной частоты КГ, увеличение индуктивности нагрузочного контура приводит к увеличению добротности КГ, уменьшение индуктивностей разрядных цепей приводит к уменьшению длительности переходного процесса при включении КГ.

2) Уменьшение общей длительности смены фазы выходного сигнала КГ приводит к увеличению значения выходного напряжения согласованного фильтра. Значение выходного напряжения согласованного фильтра достигает максимального значения при паузах между импульсами токов тиристоров КГ равных 6 мкс.

3) Вычислительный эксперимент показал совпадение расчётных зависимостей и результатов натурного эксперимента, что подтверждает адекватность разработанной математической модели и обоснованность её применения при разработке и модернизации КГ.

Литература

1. Антенно-фидерные устройства и распространение радиоволн: Учебник для вузов / Г. А. Ерохин, О. В. Чернышев, Н. Д. Козырев, В. Г. Кочержевский; под ред. Г. А. Ерохина. – М.: Горячая линия-Телеком, 2007. – 491 с.
2. Катанович А. А., Берестов С. Н., Цыванюк В. А. Принципы построения береговых систем и комплексов связи военно-морского флота. СПб.: ВМА, 2001. 406 с.
3. Бальянс Р. Х., Сиверс М. А. Тиристорные генераторы и инверторы. – Л.: Энергоиздат. Ленингр. отд-ние, 1982. – 223 с.
4. Алексеев О. А., Бунтов С. М., Егоров В. В., Наумочкин В. Ф. Анализ переходных процессов в цепях ключевого генератора с использованием его математической модели //Техника средств связи, сер. ТРС. 1981. № 5.С. 3-11.

5. Баранов А. А., Егоров В. В. Оптимизация параметров информационного сигнала СДВ диапазона // Техника средств связи. 2024. № 1 (165). С. 13-21.
6. Смит Дж. М. Математическое и цифровое моделирование для инженеров и исследователей / Пер. с англ. Н.П. Ильиной; под ред. О.А. Чембровского. М.: Машиностроение, 1980. 271 с.
7. Алексеев О. А., Егоров В. В. Численное решение системы уравнений переменных состояния для одного класса входных воздействий // Электронное моделирование. 1986. № 3. С. 85-86.
8. Радиотехнические цепи и сигналы: Учеб. Для вузов по спец. «Радиотехника»/ С. И. Баскаков. – М.: Высш. шк., 2005. – 462 с.
9. Системы широкополосной радиосвязи: учеб. Пособие для студ. Вузов / М. И. Мазурков. – Одесса: Наука и техника, 2009. – 344 с.
10. Vernay P. D. L'evolution des communications navales. // Division Telecommunications de THOMSON-CSF. 1986. № 18. P. 93-120.
11. Yamon G., Goudezeune G., Baer J.-M. Presentation des monulations a deplacement de frequence a deux etats et a phase continue d'indice 0,5 (MSK) et d'indice 1 (CPFSK) // Division Telecommunications de THOMSON-CSF. 1986. № 18. P. 156-169.

References

1. Erokhin G. A., Chernyshev O. V., Kozyrev N. D., Kocherzhevsky V. G. Antenna-Feeder Devices and Radio Wave Propagation. Moscow. Goryachaya Liniya-Telekom Publ., 2007. 491 p. (in Russian).
2. Katanovich A. A., Berestov S. N., Tsyvanyuk V. A. Principles of Building Coastal Systems and Naval Communications Complexes. St. Petersburg. Naval Academy Publ., 2001. 406 p. (in Russian).
3. Balyans R. H., Sivers M. A. Thyristor Generators and Inverters. – Leningrad: Energoizdat. Leningrad branch, 1982. 223 p. (in Russian).
4. Alekseev O. A., Buntov S. M., Egorov V. V., Naumochkin V. F. Analysis of transient processes in the circuits of a key generator using its mathematical model. *Means of Communication Equipment, ser. TRS*, 1981, no. 5, pp. 3-11 (in Russian).
5. Baranov A. A., Egorov V. V. Optimization of the parameters of the information signal of the SHF range. *Means of Communication Equipment*, 2024, no. 1 (165), pp. 13-21 (in Russian).
6. Smith J. M. Mathematical and digital modeling for engineers and researchers. Translated from English by N. P. Ilyina; edited by O. A. Chembrovsky. Moscow. Mechanical Engineering, 1980. 271 p. (in Russian).
7. Alekseev O. A., Egorov V. V. Numerical solution of the system of state variable equations for one class of input actions. *Electronic modeling*, 1986, no. 3, pp. 85-86 (in Russian).
8. Baskakov S. I. Radio engineering circuits and signals. Moscow. Vysshaya Shkola Publ., 2005. 462 p. (in Russian).
9. Mazurkov M. I. Broadband radio communication systems. Odessa. Science and Technology Publ., 2009, 344 p. (in Russian).
10. Vernay P. D. L'evolution des communications navales. *Division Telecommunications de THOMSON-CSF*, 1986, no. 18, pp. 93-120.
11. Yamon G., Goudezeune G., Baer J.-M. Presentation des monulations a deplacement de frequence a deux etats et a phase continue d'indice 0,5 (MSK) et d'indice 1 (CPFSK). *Division Telecommunications de THOMSON-CSF*, 1986, no. 18, pp. 156-169.

Статья поступила 20 июня 2026 г.

Информация об авторах

Баранов Артём Александрович – ведущий инженер АО «РИМР». Аспирант АО «РИМР». Область научных интересов: системы связи, устройства генерирования и формирования радиосигналов. Тел.: +7(911) 217-49-00 E-mail: artiom.baranov2015@yandex.ru.

Егоров Владимир Викторович – Доктор технических наук, профессор. Заведующий базовой кафедрой «Радиостроения и средств связи для телемедицины и МЧС» на базе АО «Российский институт мощного радиостроения». Санкт – Петербургский государственный университет аэрокосмического приборостроения, Институт радиотехники и инфокоммуникационных технологий. Область научных интересов: системы радиосвязи. Тел.: 8 (812)328-45-50 доб. 807.

Адрес: 199178, г. Санкт-Петербург, 11-я линия Васильевского острова, д. 66, лит. А.

Optimization of the output signal of the key range shift generator in relative phase telegraphy

A. A. Baranov, V. V. Egorov

Annotation. Problem statement: for communication with deep-submerged objects, the ultra-long wave range is usually used. Ultra-long waves propagate over distances of up to tens of thousands of km with low attenuation and are characterized by high stability of the amplitude of the field strength and phase. Radio communication in the ultra-long wave ranges is practically not accompanied by fading, and is resistant to ionospheric disturbances. Electromagnetic waves of the ultra-long wave range band propagate practically in a spherical waveguide formed by the surfaces of the Earth and the ionosphere. Due to the high value of the reactive component of the input resistance, significant reactive power is associated with the antenna, which is not involved in radiation. Therefore, the antenna efficiency does not exceed 10-30 %. For the same reason, the Q-factor of the ultra-long wave range antenna is very high, and as a result, the bandwidth is very small. Therefore, ultra-long wave range antennas are used for radiotelegraphic communication with low transmission rates. Having a relatively small electrical length, ultra-long wave range antennas have a low emissivity. Therefore, high-power transmitters are required for stable radio communication. Key thyristor harmonic oscillators, characterized by high efficiency, are used in ultra-long-wavelength radio transmission devices to generate powerful harmonic oscillations. To transmit messages, the harmonic signal is modulated according to the law of the transmitted message. When a modulated signal passes through the output circuits of the radio transmitters, transients occur, which lead to a decrease in the energy of the information signal, which in turn reduces the reliability of message transmission. The problem arises of choosing the optimal operating mode of the key thyristor harmonic oscillators, at which the energy index of the signal on the receiving side reaches its maximum value. **The purpose of the work** is to determine the dependence of the effective energy of the signal generated by the key generator of the shift range on the parameters of the circuit and the control system of the key thyristor harmonic oscillators. The thyristor harmonic oscillators operates in the relative phase telegraphy mode. **Methods used:** The study is carried out by the method of computational experiment, in which a system with a variable structure, described in each of the states by a system of differential equations, is matched to the nonlinear scheme of a thyristor KG. **The novelty:** it consists in the formalization of the process of functioning of the key thyristor harmonic oscillators by a system with a variable structure, which makes it possible to conduct a computational experiment that adequately describes the real key thyristor harmonic oscillators. **Result:** an algorithm and a program for a computational experiment have been developed that allows for a multivariate analysis of the key thyristor harmonic oscillators operation. **Practical significance:** the results of the work can be used to create a model of a key thyristor harmonic oscillators operating in the ultra-long wave ranges, which will lead to a reduction in the volume of a full-scale experiment.

Keywords: key generator, variable structure system, equivalent substitution scheme, algorithm for solving the equation of state.

Information about the authors

Artem Alexandrovich Baranov – lead engineer of RIMR JSC. Postgraduate student of RIMR JSC. Research interests: communication systems, devices for generating and generating radio signals. Tel.: +7(911)217-49-00 E-mail: artiom.baranov2015@yandex.ru.

Vladimir Viktorovich Egorov – Doctor of Technical Sciences, Professor. Head of the basic department "Radio engineering and communications for telemedicine and the Ministry of Emergencies" on the basis of JSC "Russian Institute of Powerful Radio Engineering." St. Petersburg State University of Aerospace Instrumentation, Institute of Radio Engineering and Infocommunication Technologies. Research interests: radio communication systems. Tel.: 8 (812)328-45-50 ext. 807

Для цитирования:

Баранов А. А., Егоров В. В. Оптимизация выходного сигнала ключевого генератора СДВ диапазона при относительной фазовой телеграфии // Техника средств связи. 2026. № 2 (174). С. 82-89. DOI: 10.24412/2782-2141-2026-2-82-89.

For citation:

Baranov A. A., Egorov V. V. Optimization of the output signal of the key range shift generator in relative phase telegraphy. *Means of Communication Equipment*, 2026, no. 2 (174), pp. 82-89 (in Russian). DOI:10.24412/2782-2141-2026-2-82-89.

РОБОТОТЕХНИЧЕСКИЕ СИСТЕМЫ

УДК 621.396.93

DOI: 10.24412/2782-2141-2026-2-90-100

Оценка помехоустойчивости сигнально-кодовых конструкций команд управления беспилотными транспортными средствами на основе технологий расширения спектра

Будко Д. Д.

Аннотация. Постановка задачи. Поиск приемлемых по помехоустойчивости алгоритмов построения сигнально-кодовых конструкций команд управления автономными беспилотными системами в условиях широкого их внедрения в транспортной отрасли страны. **Цель работы:** проведение экспериментальной проверки помехоустойчивости сигнально-кодовых конструкций команд управления беспилотными транспортными средствами, сформированных с использованием технологий расширения спектра. **Используемые методы:** технологии расширения спектра методом прямой последовательности, расширения спектра методом линейной частотной модуляции, а также метод перестройки рабочих частот по псевдослучайному закону в параллельном режиме. **К основным результатам** исследования можно отнести повышение помехоустойчивость командной радиолинии беспилотного транспортного средства на 15 % и на 42 % в условиях воздействия, соответственно, широкополосной и сосредоточенной помех, за счет применения сигнально-кодовых конструкций, сформированных на основе технологий расширения спектра. **Практическая значимость** предложенных результатов состоит в повышении устойчивого управления беспилотными транспортными системами как на глобальных расстояниях от их ситуационных центров, так и в крупных городских агломерациях.

Ключевые слова: линейная частотная модуляция, помехоустойчивость, перестройка рабочих частот по псевдослучайному закону, прямое расширение спектра, технологии расширения спектра.

Введение

Из теории радиосвязи хорошо известно, что методы организации радиообмена с удаленными мобильными объектами при построении сигнально-кодовых конструкций (СКК) на основе применения технологий расширения спектра преимущественно выигрывают по помехоустойчивости в сравнении с традиционными радиосигналами амплитудной (АТ) и частотной (ЧТ) телеграфии [1-5]. В более ранних работах автора [6-8] также были рассмотрены вопросы использования многочастотных сигналов для формирования СКК команд управления (КУ) глобально перемещающимися беспилотными транспортными системами (БТС) в условиях помех. Из чего был сделан вывод о положительных свойствах таких СКК как в целом по устойчивости [6], так и по оперативности [7] и информационной скрытности [8] в доведении КУ до БТС, предотвращая несанкционированный её перехват в командной радиолинии (РЛ).

Цель статьи – проведение экспериментальной проверки помехоустойчивости СКК команд управления БТС, сформированных с использованием технологий расширения спектра.

Обзор алгоритмов построения помехоустойчивых СКК команд управления БТС по технологиям расширения спектра

На сегодня, с активным внедрением в хозяйственную деятельность автономных беспилотных систем, вопросам построения помехоустойчивых СКК их команд управления посвящено множество публикаций [6-12]. Для решения подобных задач построения эффективных СКК при доведении команд управления до БТС в условиях помех [6-8, 12] чаще используют алгоритмы на основе технологий расширения спектра, например, такие как [3, 4]:

- метод линейной частотной модуляции (ЛЧМ) (CSS, Chirp Spread Spectrum);
- метод прямой последовательности (ППС), (DSSS, Direct Sequence Spread Spectrum);
- метод перестройки рабочих частот по псевдослучайному закону – ПППЧ, (FHSS, Frequency-Hopping Spread Spectrum), т. е. путем смены рабочих частот по известной только абонентам РЛ некой псевдослучайной последовательности (ПСП).

В работе [6] автором предложен алгоритм построения СКК команд управления БТС по технологии расширения спектра на базе ЛЧМ-сигналов, рис. 1, включающий процедуры:

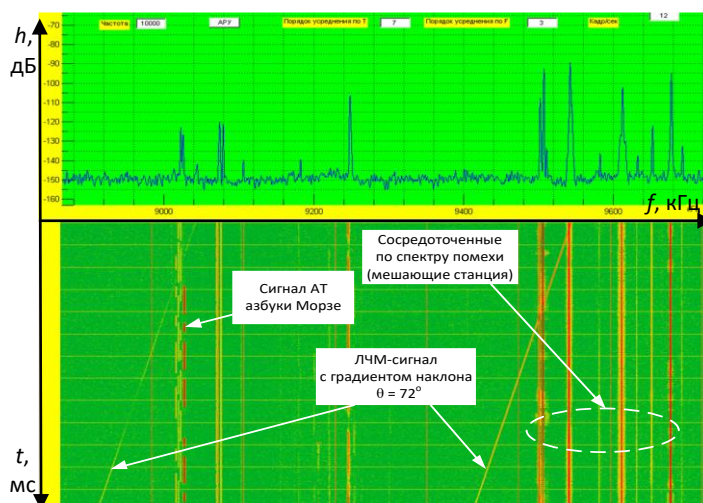


Рис. 1. Внешний вид опорного ЛЧМ-сигнала с градиентом наклона ($\theta = 72^\circ$) и сигнала АТ на реальной спектрограмме типа «Водопад» в полосе частот 8,85 – 9,75 МГц

- предварительного этапа, осуществляемого на ситуационном центре управления (СЦУ) БТС и включающим выбор его маршрута с оценкой состояния среды передачи КУ;
- этапа формирования бинарных посылок КУ, включая шаги по синтезу опорного ЛЧМ-сигнала, отрезки которого разного градиента наклона являются элементами КУ, рис. 2;
- этапа формирования каналов управления БТС;

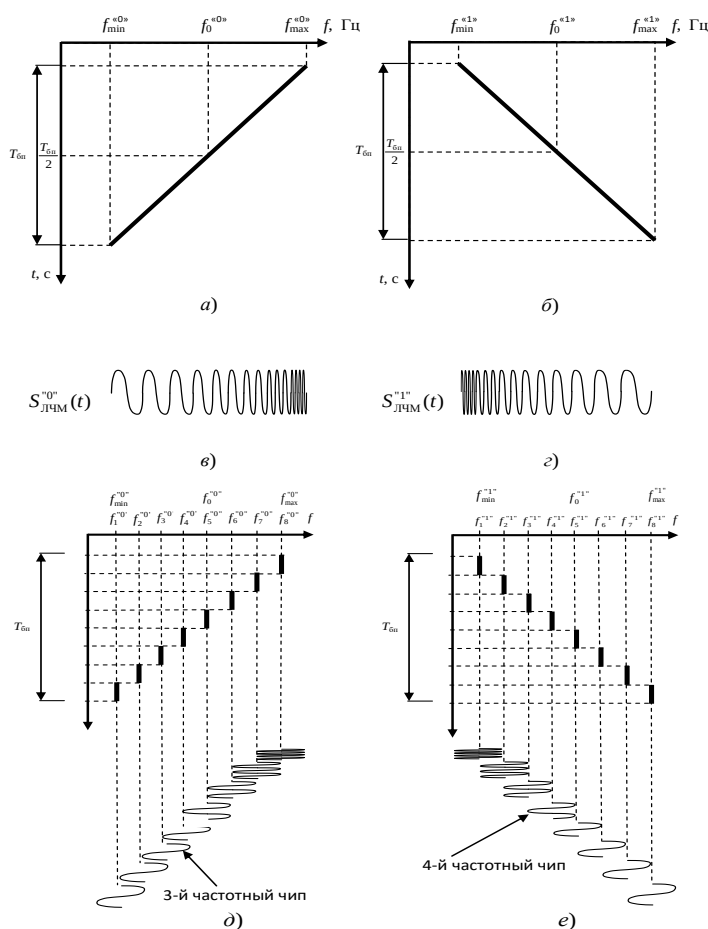


Рис. 2. Частотно-временные характеристики сигналов с расширением спектра: а) по технологии CSS с линейно возрастающим (б) законом изменения частоты; б) по технологии CSS с линейно убывающим изменением частоты (г); д) по технологии DSSS (ПРС) с дискретным возрастанием частот последующих чипов; е) по технологии DSSS с дискретным спадом частот последующих чипов

- этапа формирования СКК команды управления БТС;
- этапа доведения КУ БТС, включающего последовательную трансляцию ее элементов, а также прием, декодирование и идентификацию КУ по заданному правилу;
- завершающего этапа по доведению КУ до исполнительных устройств БТС.

Опорные ЛЧМ-сигналы бинарных посылок (бп) «0» и «1» формируются, соответственно, по выражениям, описывающим процедуры линейного убывания (1) и линейного возрастания (2) закона изменения частоты, рис. 2 а) – з):

$$S_{\text{ЛЧМ}}^{\text{''1''}}(t) = S_0 \cos\{\varphi_0 - \varphi(t)\} = S_0 \cos\{\varphi_0 - 2\pi[f_0 t + (b/2)t^2]\}, \quad (1)$$

$$S_{\text{ЛЧМ}}^{\text{''0''}}(t) = S_0 \cos\{\varphi_0 + \varphi(t)\} = S_0 \cos\{\varphi_0 + 2\pi[f_0 t + (b/2)t^2]\}, \quad (2)$$

где S_0 – амплитуда передаваемого ЛЧМ-сигнала, φ_0 – начальная фаза ЛЧМ-сигнала, $f_0 = (f_{\max} + f_{\min})/2$ – центральное значение несущей частоты ЛЧМ-сигнала, рассчитываемое, как среднее от суммы ее минимального $f_{\min}$ и максимального значения $f_{\max}$; b – параметр оценки скорости изменения частоты ЛЧМ-сигнала во времени (3), T_c – длительность ЛЧМ-сигнала

$$b = (f_{\max} - f_{\min})/T_c. \quad (3)$$

Таким образом, внутри бинарных посылок (информационных нулей «0» и единиц «1») частота во времени $f(t)$ изменяется по линейному закону с параметром b

$$f(t) = f_0 + b \cdot t, \quad (4)$$

$$-T_c/2 < t < T_c/2. \quad (5)$$

В этой же работе [6] данный алгоритм усовершенствован использованием вместо ЛЧМ-сигналов технологии расширения спектра прямой последовательностью (DSSS). При этом каждая бинарная посылка (информационная единица «1» или информационный ноль «0») КУ разбивается на несколько частотных чипов, рис. 2 д), е), передаваемых не по линейному закону (4), а в виде узкополосных сигналов, дискретно. Причем каждый из n частотных чипов передается на частотах ПСП, известной только передающей и приемной сторонам. Таким образом, для расширения спектра сигнала осуществляется перемножение исходного узкополосного сигнала на высокоскоростную ПСП. Данная технология позволяет повысить устойчивость такого широкополосного сигнала (ШПС) к узкополосным помехам.

В работах автора [7, 12] рассмотрен алгоритм формирования помехоустойчивых СКК КУ БТС методом ППРЧ (FHSS) с параллельной трансляцией информационных бит, фактически доводя процедуру доведения КУ до режима реального времени, когда за время излучения одного бита в параллельном формате доводится все сообщение (КУ). Рассмотрим процедуру повышения помехоустойчивости предложенных в работах [6, 7, 12] подробнее.

Теоретическое обоснование алгоритмов повышения помехоустойчивости

В соответствии с классическим подходом к построению СКК для РЛ, (в том числе и для РЛ декаметрового (ДКМ) диапазона волн, обеспечивающих связь с глобально удалёнными БТС) для устойчивого доведения КУ необходимо обеспечить в точке приёма соотношение мощностей сигнал/помеха не ниже заданного значения $K \geq P_s/P_n$. При этом для любого вида модуляции, если за счёт постановки преднамеренной помехи (пред.п) $K = P_s/P_{\text{пред.п}} < K$ происходит нарушение связи. Вместе с тем, если полезный сигнал не имеет специальной структуры (ШПС, ЧТ, ОФТ и т. д.), а принимается лишь по энергетическому признаку, то появление помехи на частоте приёма сигнала увеличивает его суммарную мощность и тем самым приводит к повышению вероятности приёма. Исходя из этого, предположим, что на псевдослучайной рабочей частоте f_i , неизвестной для постороннего наблюдателя (например, в режиме DSSS или FHSS) в заданный момент времени t_i (абоненту известны f_i и t_i) передается значение бита сообщения «1» путём излучения немодулированного отрезка синусоиды длительностью τ , рис. 3.

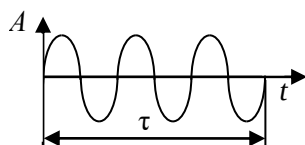


Рис. 3. Немодулированный сигнал

Приём такого сигнала, так же, как и обнаружение средствами РЭБ, может осуществляться с помощью энергетического обнаружителя, рис. 4 [1]. Следовательно, постановка помехи на неструктурированный сигнал, при оговоренных условиях лишь повысит суммарную мощность принимаемого сигнала «1», т. е. увеличит вероятность его приёма при использовании энергетического обнаружителя.

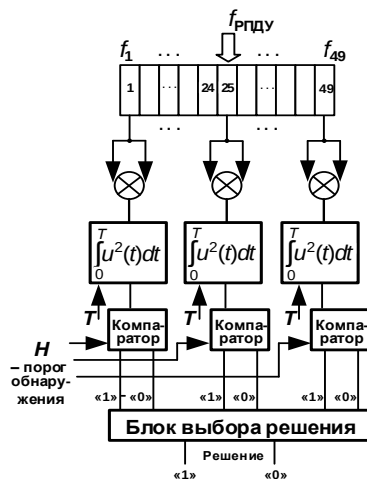


Рис. 4. Структурная схема энергетического обнаружителя

При передаче информации в режиме АТ с пассивной паузой биты со значением «0» определяются по отсутствию сигнала на заданной рабочей частоте, т.е. посторонний наблюдатель не может обнаружить сигнала и соответственно поставить сосредоточенную помеху ввиду отсутствия информации о частотах при работе в режиме ППРЧ.

Таким образом, постановка прицельных сосредоточенных помех на сообщения, передаваемые в режиме АТ, путём параллельного излучения всех бит не может снизить вероятность их приёма. Кроме того, при параллельной передаче всего текста сообщения режим АТ имеет энергетическое преимущество перед другими видами модуляции, поскольку в среднем количество единиц и нулей в тексте сообщения (команде) одинаково, мощность передачи единиц «1» может быть увеличена примерно в два раза при сохранении той же мощности передачи, что и при других видах модуляции.

Однако для эффективного функционирования энергетического обнаружителя узкополосного сигнала помимо исходных данных о начале и завершении сеанса связи он также должен получать значение оптимального порога обнаружения H , рис. 4, [1]. Значение H возможно получить, воспользовавшись выражением для средней вероятности ошибки при некогерентном приёме сигнала АТ, определяемое по формуле [13]:

$$p_{\text{ош}} = \frac{1}{2} \int_0^H \frac{2V_1}{Wv^2} \exp\left(-\frac{V_1^2 - W^2}{Wv^2}\right) I_0\left(\frac{2V_1}{v^2}\right) dV_1 + \frac{1}{2} \exp\left(-\frac{H^2}{Wv^2}\right), \quad (6)$$

где V_1 – напряжение огибающей сигнала на выходе полосового пропускающего фильтра (ППФ) $f_1 - f_{49}$ по окончании сеанса.

Оптимизировать значение порога H возможно путем минимизации вероятности ошибки $p_{\text{ош}}$, взяв производную выражения (6) и приравняв её к нулю:

$$I_0\left(\frac{2H}{v^2}\right) = \exp\left(\frac{W}{v^2}\right). \quad (7)$$

Тогда используя аппроксимацию функцией Бесселя нулевого порядка [13]:

$$I_0(z) \approx \frac{\exp(z)}{\sqrt{2\pi z}} \quad \text{при } z \geq 2 \quad (8)$$

получаем зависимость величины порога H от энергии бита сигнала W :

$$\frac{2H}{v^2} - \ln \sqrt{2\pi \frac{2H}{v^2}} = \frac{W}{v^2}. \quad (9)$$

Из проводимых в дальнейшем вычислений следует, что при $W/v^2 > 15$ дБ $H \approx W/2$. В то же время при $W/v^2 \leq 15$ дБ, что для случая решения нашей задачи в командной РЛ БТС представляет большой интерес, на значение оптимальной величины порога обнаружения в большей мере влияет мощность накопленного сигнала и v^2 . В случае отсутствия априорных данных по их значениям и ориентировочной установке величины порога H это может существенно понизить эффективность процедуры приёма. Однако, считая шумы стационарными в полосе $\Delta f \approx 10$ Гц на протяжении 20 с, значение v^2 может быть получено по предварительным их замерам за 10 секунд до начала сеанса связи. Величину энергии бита сигнала W можно оценить исходя из мощности радиопередающего устройства (РПДУ), а также конкретных условий РЛ, но при большом числе задействованных в многочастотном сигнале каналов (например, на рис. 4 в демодуляторе программно используется 49 фильтров) вероятность принятия ошибочного решения возрастет с уменьшением отношения W/v^2 . Альтернативой здесь может служить вариант определения значений дисперсии шума и среднеквадратического отклонению σ по ансамблю из 49 выборок, которые получены перед началом сеанса связи.

Так, на рис. 5 во фрагменте приема узкополосных сигналов использованы три порога H : σ , 2σ и 3σ [1, 4, 7, 8]. Значения этих порогов предоставляют декодеру дополнительно при оценке вероятности принятого решения по каждому биту КУ, что повышает помехоустойчивость приема.

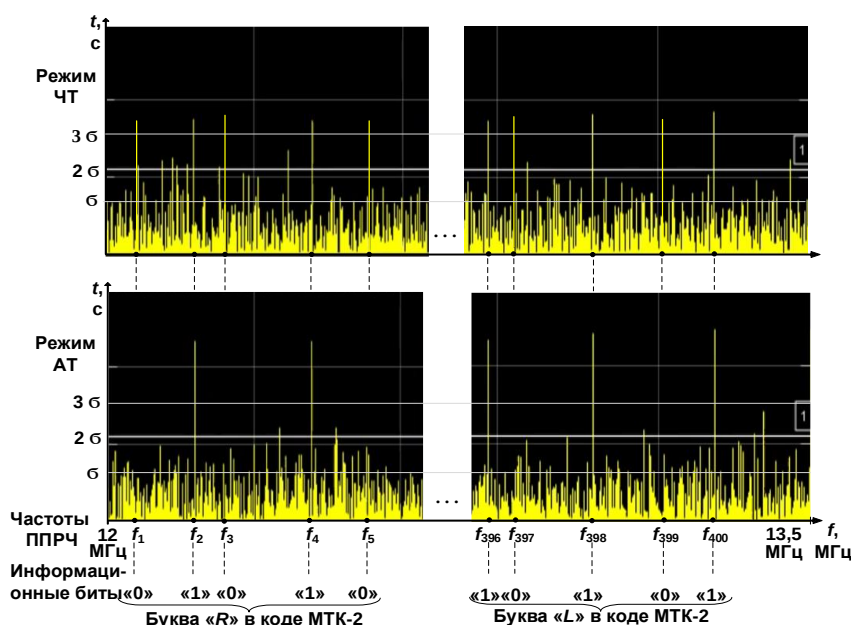


Рис. 5. Фрагменты спектрограммы СКК команды управления транслируемой в параллельном формате в режимах ЧТ и АТ при заданной мощности излучения радиопередающего устройства

Результаты проведения вычислительного эксперимента по проверке алгоритмов повышения помехоустойчивости

На рис. 5 приведены результаты вычислительного эксперимента в среде программирования *MatLab* с использованием начального и конечного фрагментов трансляции сообщения из 400 бит с приемом букв «R» и «L» в коде МТК-2 для режимов АТ и ЧТ. При этом в случае параллельной трансляции информационных бит КУ важно учитывать, что для каждой бинарной посылке при приёме с заданной вероятностью необходимо обеспечить определённое значение параметра оценки помехоустойчивости $h^2 = P_c T / v^2$, где P_c – мощность излучения бита сообщения, T – длительность бита сообщения, v^2 – спектральная плотность шума. [1, 13]. Из чего следует, что при параллельной передаче бит без учета пик-фактора сигнала с сохранением общей мощности излучения РПДУ потребуется в N раз увеличить время излучения каждого бита. Например, если последовательно передавалась команда их $N = 1000$ бит с длительностью $\tau = 10$ мс, то для сохранения значения h^2 при параллельной передаче длительность излучения

одного бита должна быть не менее $tN \approx 10$ с. Причем время передачи всей КУ в обоих случаях будет примерно одинаковым $T_{\text{сванс}} \approx 10$ с, если не учитывать время на перестройку частот в радиоприёмном устройстве (РПУ) при последовательной передаче бит.

При этом частотная полоса, занимаемая «длинным» сигналом, составит примерно $\Delta f \approx 1/10 \text{ с} = 0,1 \text{ Гц}$. Обнаружение таких «сверхузкополосных» сигналов средствами РЭБ при отсутствии знания рабочих частот представляется проблематичным, поскольку для этого потребуется значительное количество независимых каналов приёма в обнаружителе, а также большое время накопления сигнала для его достоверной идентификации.

На рис. 6 приведены фрагменты спектрограмм, характеризующих выделение параллельно передаваемых сверхузкополосных сигналов из-под шумов в режиме параллельной ППРЧ, где за время трансляции одного бита передается вся КУ. При этом можно отметить, что процесс «накопления» сигнала является вполне равномерным, а наличие сигнала в канале определяют по росту градиента напряжения огибающей на выходе каждого канального ППФ. Однако, такой алгоритм требует значительных вычислительных ресурсов.

Проведение экспериментальных исследований в реальных условиях ДКМ радиосвязи, подтвержденное результатами имитационного моделирования, показало, что $15 \div 25 \%$ сообщения для рассматриваемой СКК будут приняты с ошибками из-за наличия медленных замираний сигнала и сосредоточенных помех на рабочих частотах. Учитывая это, дополнительно в работе предлагается использование помехоустойчивых кодов. Обычно в ДКМ РЛ используется недвоичный циклический код Рида-Соломона (n, k) , исправляющий до $t = (n - k)/2$ ошибок в блоке КУ, где k – число бит КУ, n – число символов в кодируемом блоке.

Тогда, если $t \approx 0,25n$, то максимальная скорость кода будет достаточно низкой: $R \approx 1/2$. В таких случаях будет более эффективным использовать коды Рида-Соломона на каскадных схемах кодирования [14]. При этом важно учитывать, что при демодуляции сигнала с использованием нескольких порогов обнаружения сигналов (на рис. 5: $H = \sigma \div 3\sigma$) каждому биту КУ может быть дана вероятностная оценка. Это позволяет целесообразным рассмотреть и другие эффективные методы кодирования/декодирования информации, включая использование итеративных алгоритмов и каскадных кодов с «мягким» решением.

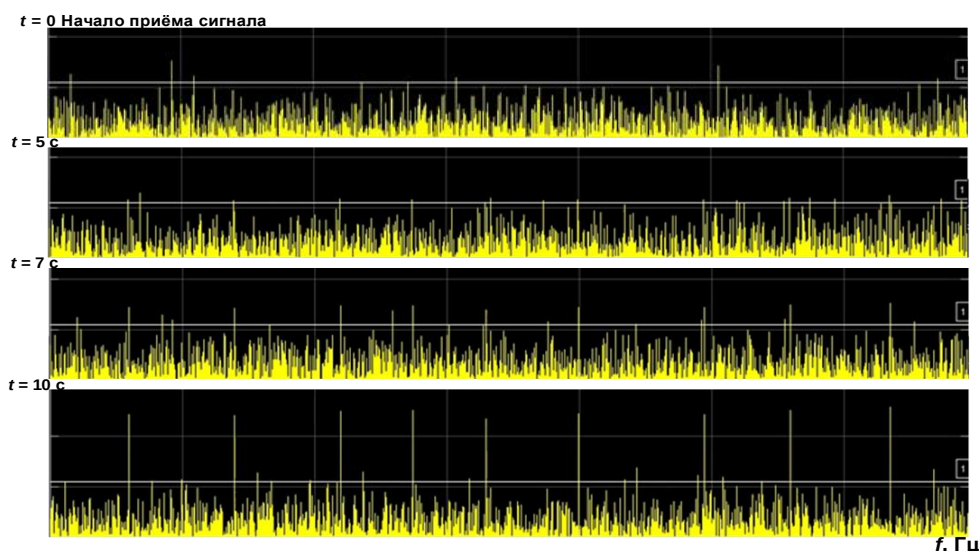


Рис. 6. Временные диаграммы фрагмента спектрограмм приема информационных бит посылок элементов КУ в многочастотном сигнале в ходе вычислительного эксперимента

Рассмотренные алгоритмы формирования СКК позволяют обеспечить приём не только в шумах, рис. 7 а), и сосредоточенных помехах рис. 7 б), но также и организовать мероприятия по уходу от мощных широкополосных помех, рис. 7 в). Для различной помеховой обстановки возможно адаптировать соответствующий алгоритм. Например, под широкополосной помехой, приведенной на рис. 7 в) наиболее приемлема СКК на основе ЛЧМ, а не на основе ПРС и ППРЧ.

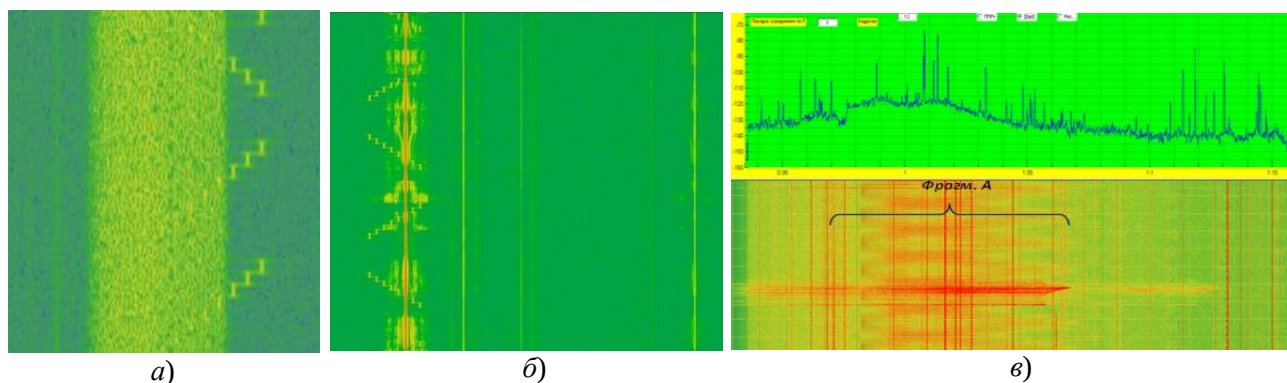


Рис. 7. Фрагмент СКК, полученной на основе применения технологии ПРС в шумах – а) и под сосредоточенной помехой – б). Мощная широкополосная помеха во фрагменте А – в)

При возникновении сложной помеховой ситуации с блокирующей весь диапазон широкополосной помехой в работе [12] автора было представлен вариант обеспечения устойчивого доведения КУ до глобально перемещающихся БТС за счет комплексного использования радиочастотного спектра (РЧС), с уходом в другую полосу частот или диапазон.

Перед постановкой такого вида помех программно-аппаратные комплексы мониторинга РЧС бортового комплекса связи (БКС) БТС и СЦУ должны с малой вероятностью ложной тревоги (л.т.) обнаружить начало работы РЛ. При этом обнаружение узкополосных сигналов рассматриваемой в работе структуры требует в БКС БТС размещения модуля параллельного поиска минимум на $1/5 \cdot \Delta F_{\text{ППРЧ}}$ для обнаружения момента начала одновременного излучения многочастотного сигнала. Для рассматриваемой СКК, излучаемой в полосе $\Delta F_{\text{ППРЧ}} \approx 1$ МГц и $\Delta f \approx 0,2$ Гц, даже если предположим, что поиск сигналов посторонним наблюдателем проводится в полосе $\Delta f_{\text{сигн}} = 0,5$ Гц (что значительно понизит вероятность обнаружения сигнала из-за увеличения отношения сигнал/помеха – P/P_n), при контроле заданной полосы частот необходимо минимум сотни тысяч каналов параллельного приема: $K = \frac{1}{5} \frac{\Delta F_{\text{ППРЧ}}}{\Delta f_{\text{обн}}} \approx 400\,000$ кан.

По формуле Бернулли легко убедиться, что в таком случае даже при достаточно малой вероятности ложной тревоги в одном канале, например, $P_{\text{л.т.}} \approx 10^{-5}$, суммарная вероятность ложной тревоги будет очень высокой. Пусть даже потенциальному нарушителю удалось до окончания сеанса связи осуществить приём и классификацию сигнала с поставкой на него помехи, но учитывая, что командная РЛ обладает дополнительной информацией по рабочим частотам и времени сеанса (матрица ППРЧ, матрица псевдослучайного времени сеансов связи), а также то, что в ней используются оптимизированные по диаграммам направленности фазированные антенные решетки под абонентов РЛ, а рабочие частоты взяты из области оптимальных рабочих частот, можно допустить, что к началу воздействия помехи, РПУ БКС БТС имеет возможность принять и демодулировать сигнал. Для этого ключевым условием будет прекращение «накопления» сигналов в момент начала воздействия помехи. Эта задача в РЛ решается путем удвоения числа каналов приёма в бортового РПУ. Полоса частот анализа мощности помех может составлять 20-30 Гц в дополнительных каналах приема, структура расположения которых $f_{\text{дi}}$ понятна из приведённых схемных решений на рис. 8.

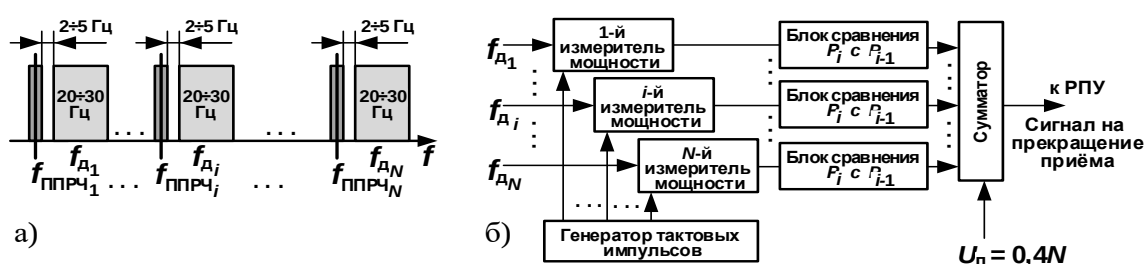


Рис. 8. Структура расположения дополнительных каналов приёма – а), структурная схема обнаружителя широкополосной блокирующей помехи – б)

Сигнал с каждого дополнительного канала-фильтра (ППФ) поступает на измеритель мощности помехи, в котором данные обновляются через $t_{\text{обн.}} \approx 50$ мс, по сигналу от момента начала сеанса связи. В блоке сравнения текущее значение мощность помехи P_i сравнивают с мощностью помехи предыдущего шага измерения $i-1$, и если $P_i > 2P_{i-1}$, в сумматор поступает сигнал управления «1». Если в сумматор одновременно поступают сигналы «1» от $K \geq 0,4N$ каналов, значит число поражённых каналов выше исправляющей способности принятого в РЛ помехоустойчивого кода, тогда от сумматора в РПУ передаётся запрещающий сигнал на продолжение приёма, и разрешающий – для перехода к демодуляции и декодированию КУ.

Оценка эффективности работы радиолинии

Оценка эффективности работы радиолинии ранее была рассмотрена в [5-8, 12, 14]. В то же время на рис. 9 представлена зависимость вероятности правильного приёма бита сообщения $p_{\text{пр}}$ для трассы длиной 6 тыс. км при мощности излучения 10 Вт и различных скоростях передачи V . На рис. 10 показаны экранные формы наследованной СКК «Азбука Морзе» и новой СКК, построенной по технологии расширения спектра при различных соотношении сигнал/помеха.

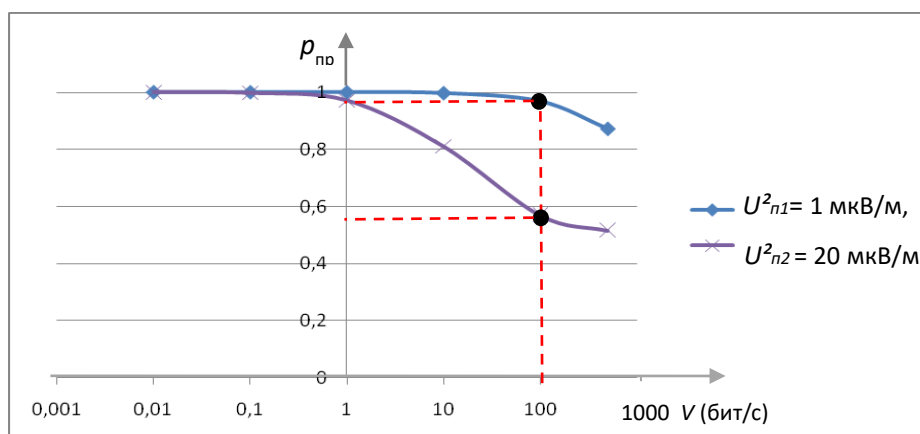


Рис. 9. Вероятность правильного приема бита КУ для трассы протяженностью 6 тыс. км, $P_{\text{изл}}=10$ Вт

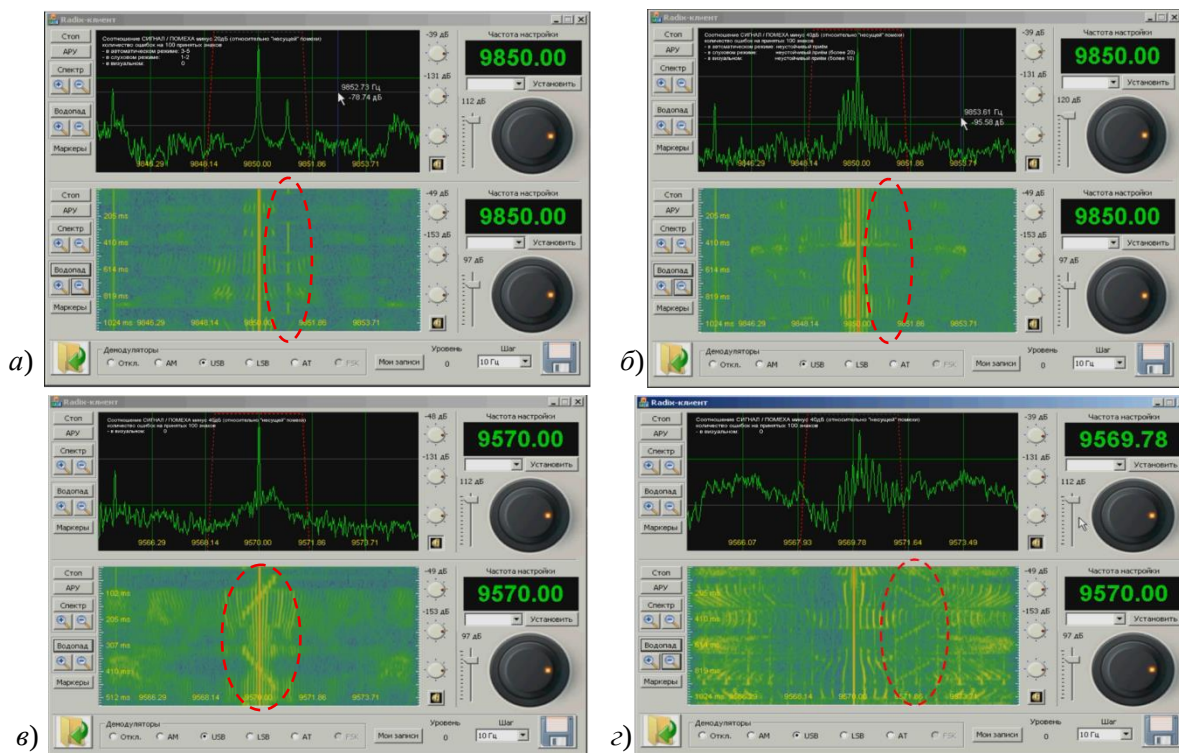


Рис. 10. Экранные формы, подтверждающие повышение помехоустойчивости предложенной СКК

В табл. 1 приведены результаты эксперимента по доведению 100 знаков КУ для наследованной СКК в коде Морзе и предложенной СКК, построенной по технологии DSSS.

В табл. 2 показана вероятность безошибочного приема КУ из 40 знаков в условиях воздействия сосредоточенной и широкополосной помех для режима параллельной ППРЧ.

Таблица 1 – Количество ошибочно принятых знаков из 100 переданных в условиях помех

Режим приема	Уровень несущей помехи минус 20 дБ		Уровень несущей помехи минус 40 дБ	
	Рис. 10 а), код Морзе	Рис. 10 в), СКК DSSS	Рис. 10 б), код Морзе	Рис. 10 г), СКК DSSS
Слуховой	1 – 2	–	Более 20	–
Визуальный	0	Устойчивый приём	Более 10	Устойчивый приём
Автоматический	3 – 5	Устойчивый приём	Неустойчивый приём	Устойчивый приём

Таблица 2 – Вероятность безошибочного приема (доведения) КУ из 40 знаков в условиях помех

Вид помехи	Приём штатного кода Морзе			Приём СКК на базе ППРЧ, рис. 6	
	Слуховой	Визуальный	Автоматический	Визуальный	Автоматический
Сосредоточенная	0,67	0,73	0,57	≈ 1,0. Из 40 переданных знаков КУ 100 % приняты	0,99
Широкополосная	0,83	0,92	0,71	0,98	0,86

Выводы

Проведенные сравнительные натурные испытания показали высокую эффективность использования визуального и автоматического приема предложенных СКК на основе технологий расширения спектра, а использование различных режимов приема информации позволяет существенно поднять помехоустойчивость ДКМ радиосвязи в условиях случайных и преднамеренных помех, а также авроральных возмущениях ионосферы в приполярных районах.

Как видно из табл. 1 и 2, применение СКК на основе методов CSS и DSSS обеспечивает устойчивый прием КУ в автоматическом режиме бортовым комплексом связи БТС, а использование автоматического приема предложенных СКК на основе параллельной ППРЧ по сравнению с штатным кодом Морзе повышает помехоустойчивость командной РЛ на 15 % и на 42 %, соответственно, в условиях воздействия на РЛ широкополосной и сосредоточенной помех.

Разработка эффективных методов обнаружения и приёма узкополосных сигналов с низкой энергетикой представляет теоретическое и практическое значение на фоне активного внедрения в транспортную отрасль страны и в хозяйственную сферу огромного числа БТС. Для повышения эффективности автоматического приема КУ БТС необходимы дополнительные исследования по внедрению в данный процесс технологий искусственных нейронных сетей (ИНС) и ИНС-платформ, что является направлением дальнейших исследований.

Литература

1. Куприянов А. И. Радиоэлектронная борьба. – М.: Вузовская книга, 2013. – 359 с.
2. Иванов М. С., Афонин И. Е., Макаренко С. И. Повышение устойчивости автоматизированной систему управления комплекса с беспилотными летательными аппаратами в условиях воздействия средств физического и радиоэлектронного подавления // Системы управления, связи и безопасности. 2022. № 2. С. 92-134. DOI: 10.24412/2410-9916-2022-2-92-134.
3. Макаренко С. И., Иванов М. С., Попов С. А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. Монография. – СПб.: Свое издательство, 2013. – 166 с. ISBN 978-5-4386-0166-1.
4. Борисов В. И., Зинчук В. М., Лимарев А. Е. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты // под ред. В. И. Борисова. М.: РадиоСофт, 2008. – 512 с.
5. Николашин Ю. Л., Будко П. А., Жолдасов Е. С., Жуков Г. А. Перспективные методы повышения помехоустойчивости декаметровых радиолоний // Научные технологии в космических исследованиях Земли. 2014. Т. 6. № 1. С. 30-37.

6. Будко Д. Д., Будко П. А., Зацепин Т. А., Клименко А. Д. Метод управления беспилотными транспортными системами на основе помехоустойчивых сигнально-кодовых конструкций в условиях сосредоточенных и шумовых помех // Системы управления, связи и безопасности. 2025. № 4. С. 143-178. DOI: 10.24412/2410-9916-2025-4-143-178.

7. Будко Д. Д., Каретников В. В. Модель формирования многочастотных сигналов команд управления беспилотных транспортных систем в условиях помех // Системы управления, связи и безопасности. 2026. № 1. С. 182-218. DOI: 10.24412/2410-9916-2026-1-182-218.

8. Будко Д. Д., Будко П. А., Каретников В. В., Клименко А. Д. Обеспечение информационной скрытности при доведении команд управления до беспилотных транспортных систем // Системы управления, связи и безопасности. 2026. № 2. С. 197-217. DOI: 10.24412/2410-9916-2026-2-197-217.

9. Макаренко С. И., Козлов К. В. Автоматизированная система управления совместными действиями морских робототехнических комплексов, безэкипажных судов и катеров // Системы управления, связи и безопасности. 2026. № 1. С. 1-34. DOI: 10.24412/2410-9916-2026-1-001-034.

10. Медведев И. М., Медведев М. Ю., Пшихопов В. Х. Алгоритмы группового управления подводными подвижными объектами // Подводные исследования и робототехника. 2024. № 3. С. 38-51.

11. Чертова О. Г., Новак К. В. Возможные способы организации связи при построении сети морских робототехнических комплексов // Научные технологии в космических исследованиях Земли. 2017. Т. 9. № 4. С. 54-61.

12. Будко Д. Д. Обеспечение устойчивого доведения команд управления до беспилотных транспортных систем за счет комплексного использования радиочастотного спектра // Техника средств связи. 2026. № 1 (173). С. 95-99. DOI: 10.24412/2782-2141-2026-1-95-99.

13. Коржик В. И., Финк Л. М., Щелкунов К. Н. Расчет помехоустойчивости систем передачи дискретных сообщений: Справочник. М.: Радио и связь, 1981. 232 с.

14. Николашин Ю. Л., Будко П. А., Жуков Г. А., Угрик Л. Н. Новое направление создания помехоустойчивых радиолний декаметрового диапазона волн // Техника средств связи. 2021. № 1. С. 2-27.

References

1. Kupriyanov A. I. *Radioe`lektronnaya bor`ba* [Electronic warfare]. Moscow. Vuzovskaya kniga publ., 2013, 360 p. (in Russian).

2. Ivanov M. S., Afonin I. E., Makarenko S. I. Increasing stability of the control system of unmanned aerial vehicles in the conditions of the damage and electronic warfare. *Systems of Control, Communication and Security*, 2022, no. 2, pp. 92-134 (in Russian). DOI: 10.24412/2410-9916-2022-2-92-134.

3. Makarenko S. I., Ivanov M. S., Popov S. A. Noise immunity of communication systems with pseudorandom frequency adjustment. The monograph. – St. Petersburg. Svoey publishing house, 2013. 166 p. ISBN 978-5-4386-0166-1.

4. Borisov V. I., Zinchuk V. M., Limarev A. E. Noise immunity of radio communication systems with signal spectrum expansion by pseudorandom frequency tuning // edited by V. I. Borisov. Moscow: RadioSoft, 2008. 512 p.

5. Nikolashin Yu. L., Budko P. A., Zholdasov E. S., Zhukov G. A. Promising methods for increasing the noise immunity of decameter radio lines. *H&ES Research*, 2014, vol. 6, no. 1, pp. 30-37 (in Russian).

6. Budko D. D., Budko P. A., Zatsepin T. A., Klimenko A. D. A method for controlling unmanned transport systems based on noise-resistant signal-code structures in conditions of concentrated and noisy interference. *Systems of Control, Communication and Security*, 2025, no. 4, pp. 143-178 (in Russian). DOI: 10.24412/2410-9916-2025-4-143-178.

7. Budko D. D., Karetnikov V. V. A model for generating multi-frequency control command signals for unmanned transport systems under interference conditions. *Systems of Control, Communication and Security*, 2026, no. 1, pp. 182-218 (in Russian). DOI: 10.24412/2410-9916-2026-1-182-218.

Budko D. D., Budko P. A., Karetnikov V. V., Klimenko A. D. Preventing unauthorized access to the control path of unmanned transport systems. *Systems of Control, Communication and Security*, 2026, no. 2, pp. 197-217 (in Russian). 197-217. DOI: 10.24412/2410-9916-2026-2-197-217.

9. Makarenko S. I., Kozlov K. V. Automated control system for joint actions of marine robotic complexes and unmanned vessels. *Systems of Control, Communication and Security*, 2026, no. 1, pp. 1-34 (in Russian). DOI: 10.24412/2410-9916-2026-1-001-034

10. Medvedev I. M., Medvedev M. Y., Pshikhov V. Kh. Algorithms for group control of underwater mobile objects. *Underwater investigations and robotics*, 2024, vol. 49, no. 3, pp. 38-51 (in Russian).

11. Chertova O. G., Novak K. V. Possible ways of organization a communication in the construction networks of marine robotic complexes. H&ES Research, 2017, vol. 9, no. 4, pp. 54–61 (in Russian).

12. Budko D. D. Ensuring sustainable delivery of control commands to unmanned transport systems due to integrated use of radio frequency spectrum. Means of communication equipment. 2026. № 1 (173). С. 95-99 (in Russian). DOI: 10.24412/2782-2141-2026-1-95-99.

13. Korzhik V. I., Fink L. M., Shchelkunov K. N. Calculation of noise immunity of discrete message transmission systems. Handbook. Moscow. Radio and Communications Publ., 1981, 232 p. (in Russian).

14. Николашин Ю. Л., Будко П. А., Жуков Г. А., Угрик Л. Н. Новое направление создания помехоустойчивых радиолиний декаметрового диапазона волн // Техника средств связи. 2021. № 1 (153). С. 2-26.

Статья поступила 15 июня 2026 г.

Сведения об авторе

Будко Дмитрий Дмитриевич – аспирант. Государственный университет морского и речного флота имени адмирала С. О. Макарова. Область научных интересов: методы управления беспилотными транспортными системами. Тел.: +7-999-204-10-62. E-mail: budd.85@yandex.ru.

Адрес: 198035, г. Санкт-Петербург, ул. Двинская, д. 5, корп. 7.

Evaluation of the noise immunity of signal-code structures of unmanned vehicle control commands based on spectrum expansion technologies

D. D. Budko

Annotation. Setting the task. The search for algorithms acceptable in terms of noise immunity for constructing signal-code structures for controlling autonomous unmanned systems in the context of their widespread implementation in the country's transport industry. **The purpose of the work:** to conduct an experimental verification of the noise immunity of signal-code structures of control commands for unmanned vehicles, formed using spectrum expansion technologies. **Methods used:** technologies of spectrum expansion by direct sequence method, spectrum expansion by linear frequency modulation method, as well as a method of adjusting operating frequencies according to a pseudorandom law in parallel mode. **The main results** of the study include an increase in the noise immunity of the command radio link of an unmanned vehicle by 15% and 42% under conditions of exposure, respectively, to broadband and concentrated interference, through the use of signal-code structures based on spectrum expansion technologies. **The practical significance** of the proposed results is to increase the sustainable management of unmanned transport systems both at global distances from their situational centers and in large urban agglomerations.

Keywords: linear frequency modulation, noise immunity, pseudorandom frequency tuning, direct spectrum expansion, spectrum expansion technologies.

Information about author

Dmitry Dmitrievich Budko – Postgraduate. State University of the Sea and River Fleet named after Admiral S.O. Makarov. Research interests: methods of managing unmanned transport systems. E-mail: budd.85@yandex.ru. Address: 198035, Russia, Saint-Petersburg, Dvinskaya St., 5/7.

Для цитирования

Будко Д. Д. Оценка помехоустойчивости сигнально-кодовых конструкций команд управления беспилотными транспортными средствами на основе технологий расширения спектра // Техника средств связи. 2026. № 2 (174). С. 90-100. DOI: 10.24412/2782-2141-2026-2-90-100.

For citation:

Budko D. D. Evaluation of the noise immunity of signal-code structures of unmanned vehicle control commands based on spectrum expansion technologies. *Means of Communication Equipment*, 2026, no. 2(174), pp. 90-100 (in Russian). DOI:10.24412/2782-2141-2026-2-90-100.

Решением ВАК № 222-р от 10 июня 2024 года

научно-технический журнал «Means of Communication Equipment» («Техника средств связи») включен в перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук (Перечень*) и рекомендован Высшей аттестационной комиссией для публикаций основных результатов по научным специальностям**:

2.2.13. Радиотехника, в том числе системы и устройства телевидения (технические науки);

2.2.14. Антенны, СВЧ устройства и их технологии (технические науки);

2.2.15. Системы, сети и устройства телекоммуникаций (технические науки);

2.3.1. Системный анализ, управление и обработка информации, статистика (технические науки);

2.3.5. Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей (технические науки);

2.3.6. Методы и системы защиты информации, информационная безопасность (технические науки).

* В Перечне от 30.03.2026 под номером 90.

** В соответствии с номенклатурой, утвержденной приказом Министерства науки и высшего образования Российской Федерации от 24 февраля 2021 г. N 118 и рекомендацией Президиума Высшей аттестационной комиссии N 15/1-нс от 28 мая 2021 г.

Индексы ГРНТИ:

20.00.00 Информатика.

28.00.00 Кибернетика.

45.00.00 Электротехника.

47.00.00 Электроника. Радиотехника.

47.05.00 Теоретическая радиотехника.

47.41.00 Радиоэлектронные схемы.

47.51.39 Синтез и обработка телевизионных сигналов.

49.00.00 Связь.

49.03.05 Теория обработки сигналов в системах связи.

49.27.00 Система передачи.

49.31.00 Многоканальная связь.

49.39.00 Телефонная связь и аппаратура.

49.43.00 Радиосвязь и радиовещание.

50.00.00 Автоматика. Вычислительная техника.

49.33.35 Надежность сетей связи и защита информации.

50.37.23 Защита от несанкционированного доступа. Физическая защита информации.

50.41.27 Компьютерные вирусы. Антивирусные программы.

81.93.29 Информационная безопасность. Защита информации