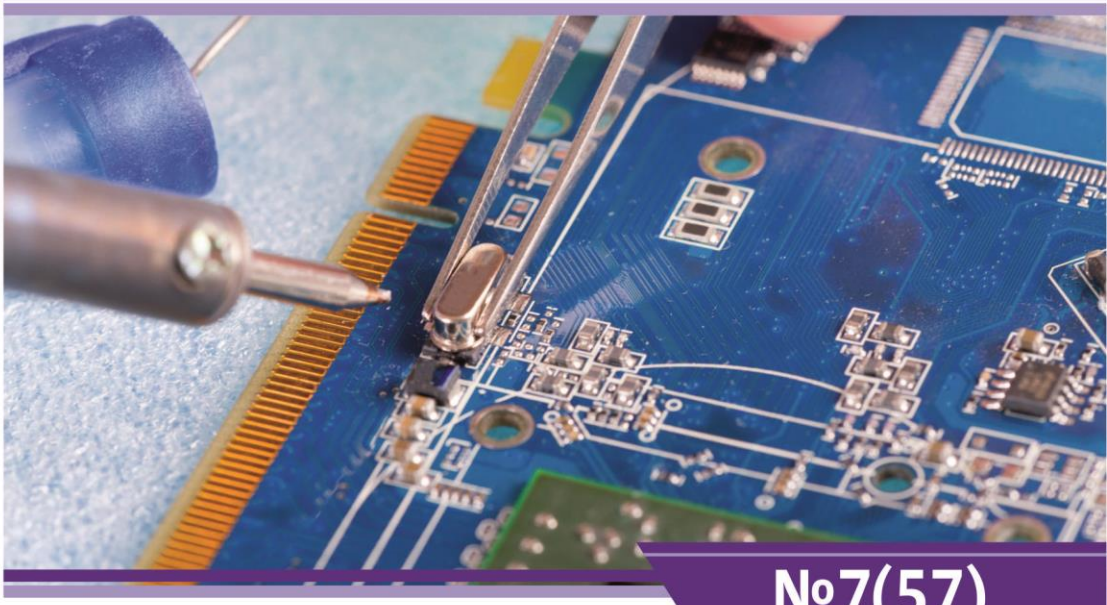
НАУЧНЫЙ ФОРУМ
nauchforum.ru

ISSN: 2541-8394



№7(57)

НАУЧНЫЙ ФОРУМ: ТЕХНИЧЕСКИЕ И ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ

МОСКВА, 2022

НАУЧНЫЙ ФОРУМ: ТЕХНИЧЕСКИЕ И ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ

Сборник статей по материалам LVII международной научно-практической конференции

№ 7 (57)
Октябрь 2022 г.

Издается с декабря 2016 года

Москва
2022

УДК 51/53+62
ББК 22+3
Н34

Н34 Научный форум: Технические и физико-математические науки: сб. ст. по материалам LVII междунар. науч.-практ. конф. – № 7 (57). – М.: Изд. «МЦНО», 2022. – 62 с.

ISSN 2541-8394

Статьи, принятые к публикации, размещаются на сайте научной электронной библиотеки eLIBRARY.RU.

ББК 22+3
ISSN 2541-8394

Оглавление

РАЗДЕЛ 1.

ТЕХНИЧЕСКИЕ НАУКИ

1.1. ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ДАННЫХ В ОПЕРАЦИОННОЙ СИСТЕМЕ ПУТЕМ ШИФРОВАНИЯ И АРХИВИРОВАНИЯ

Очилов Низомиддин Нажмиддин угли
главный специалист, программист,
Государственный центр тестирование
при Кабинете Министров,
Республика Узбекистан, г. Ташкент

ENSURING DATA PROTECTION IN THE OPERATING SYSTEM BY ENCRYPTION AND ARCHIVING

Nizomiddin Ochilov
Chief specialist, programmer,
State testing center under the Cabinet of Ministers,
Republic of Uzbekistan, Tashkent

Аннотация. Статья посвящена организации защиты данных в операционной системе посредством шифрования и архивирования в операционных системах с открытым кодом. А также она посвящена организации шифрования и дешифрования системных файлов в процессе инициализации, разработке графических программных обеспечений шифрования для файловой системы и оценке эффективности функционирования графического программного комплекса. Для отдела инициализации целостность данных важнее, чем конфиденциальность ваших данных. Метод шифрования LUKS (Linux Unified Key Setup) служит для устранения таких недостатков (рис.1). Одним из основных преимуществ является то, что зашифрованный раздел трудно подделать [1].

Abstract. The article is devoted to the organization of data protection in the operating system through encryption and archiving in open source operating systems. And also it is devoted to the organization of encryption and decryption of system files during the initialization process, the development of graphical encryption software for the file system and the evaluation of the effectiveness of the graphical software package. Data integrity is more important to the provisioning department than the privacy of your data. The LUKS (Linux Unified Key Setup) encryption method serves to eliminate such shortcomings (Fig. 1). One of the main advantages is that the encrypted partition is difficult to forge.

Ключевые слова: хеширования; шифрования; дешифрования; файловая система; криптографический модуль.
Keywords: hashing; encryption; decryption; file system; cryptographic module.

Введение. Рассмотрим возможность использования TPM (Trusted Platform Module) для хранения ключа шифрования и проверки безопасной среды загрузки. TPM на самом деле является криптопроцессором в системе. Эта технология позволяет выполнять безопасное шифрование в системе без необходимости ввода ключа (например, используя вход по отпечатку пальца или метод аутентификации, не зависящий от метода шифрования). В идеале он должен работать с UEFI Secure Boot, который, в свою очередь, не позволяет выполнять расшифровку при повреждении системных настроек.

Рисунок 1. Изображение. Метод шифрования LUKS (Linux Unified Key Setup)

Однако поддержка TPM в Linux все еще находится в зачаточном состоянии. Мы используем UEFI Secure Boot, чтобы полностью покрыть цепочку инициализации электронной подписью.

Поскольку локальный стандарт шифрования O'zDSt 1105:2009 имеет тот же размер ключа, что и AES-256, было принято решение не менять порядок генерации ключей из последовательности паролей. Для этого 7zip использует алгоритм хеширования SHA-2. Причина, по которой он имеет хорошую статистическую криптостойкость заключается в том, что он используется в качестве генератора псевдослучайных последовательностей.

Однако процедура расширения коммутатора кардинально отличается для AES и местного стандарта. Поэтому весь модуль, находящийся в файле AES.c, был модифицирован encrytp.c. 7zip осуществляет разбиение текста на 128-битные блоки и заполнение их до нужной длины в соответствии с правилами. encryptp.c модуль изменяет размер блока на 64 бита, поскольку число 128 является 64 кратным. А также это изменение не только осуществляет изменению константы, но и удваивает количество блоков [2-3].

7zip использует шифрование в режиме CBC (режим слияния зашифрованных текстовых блоков), но можно использовать и режим счетчика. Этот же метод был учтен при создании модуля encryptp.c. Поскольку функция расширения ключа изначально была заполнена раундовыми ключами с использованием встроенного уникального свойства пользовательского массива, созданного 7zip, была создана только одна раундовая функция шифрования (осуществляется во время шифрования и дешифрования).

Этот метод используется в разных режимах. В большинстве случаев отклонения во времени запуска в зависимости от выбранного режима незначительны. В режимах CBC и CFB (режим обратной связи шифротекста) время запуска увеличивается. При выборе шифрования в режиме CBC для данного метода обеспечивается криптостойкость [4].

Для оценки эффективности работы системы информационной безопасности при проведении эксперимента по выполнению файла с расширением «exe» 1, 2, 5 и 10 раз в секунду на процессоре с заданной частотой система информационной безопасности строилась в встроенном и неустановленном режимах. Для каждого значения частоты выполнения файла выполнялось по 10 экспериментов, после чего вычислялась ошибка результата измерения.

Основная часть. Для обработки результатов эксперимента были предприняты следующие шаги:

1) Среднее значение 10 тестов рассчитывается по следующей формуле:

$$x_{\text{о}} = \frac{\sum_{i=1}^{N} x_i}{N}$$

2) Ошибка рассчитывалась по следующей формуле:

$$\Delta x_i = |x_{\text{о}} - x_i|$$

3) Квадратичные ошибки вычислялись по следующей формуле.

4) Средние квадратичные ошибки среднего арифметического рассчитываются по следующей формуле:

$$S_{x_{\text{о}}} = \sqrt{\frac{\sum(\Delta x_i)^2}{n(n-1)}}$$

5) Значение надежности измерения было равно 0,95.

6) Для значения, полученного из достоверности измерения и количества проведенных экспериментов, был определен коэффициент Стьюдента t = 2,262.

7) Доверительный интервал (ошибка измерения) определялся по следующей формуле:

$$\Delta x = S_{x_{\text{ў}}} \times t$$

Из таблицы известно, что дополнительная загрузка центрального процессора в приложениях не превышает 19%. В первом эксперименте это значение не превышало 23%. Из этого можно сделать вывод, что полученная модель и результаты верны, а использование центрального процессора можно предсказать на основании результатов, которые мы привели выше.

При этом время загрузки для защищенной файловой системы увеличилось с 5 до 8 секунд, для программы записи внешних устройств – с 4 до 8 секунд, а для графического программного обеспечения шифрования для файловой системы – с 5 до 7 секунд. Время запуска полной СИБ увеличилось до 4 секунд.

Определена эффективность средств защиты и изучено влияние операционной системы на загрузку вычислительных ресурсов, при этом дополнительная загрузка процессора в режиме запуска приложений не превышала 23%, а в обычном режиме работы программ не превышала 17%, при этом время запуска программы не превышало 4 секунд (Рис.2.).

Адекватность полученных результатов доказано статистической обработкой эксперимента.

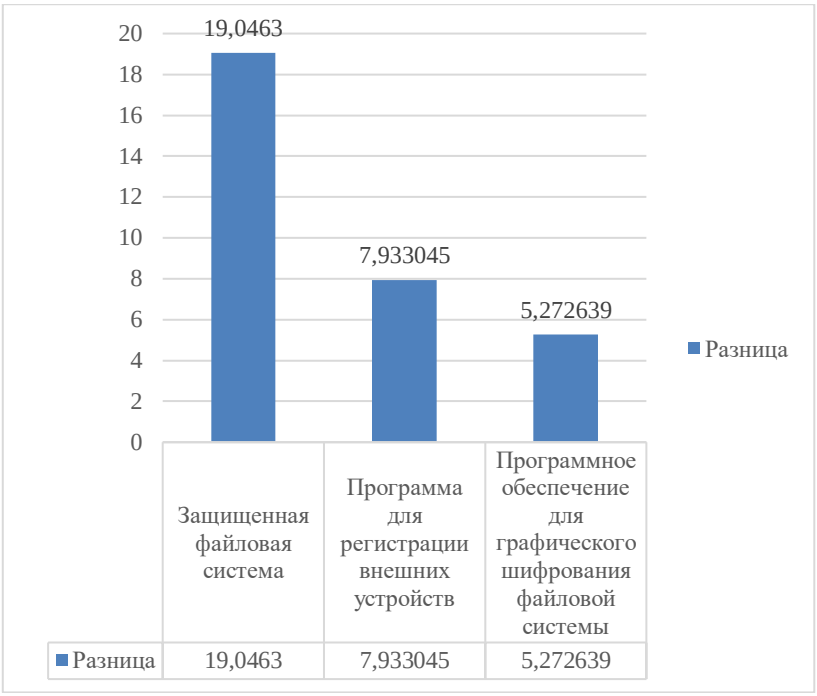


Рисунок 2. Средние квадратичные результаты производительности разработанных программ

Программное обеспечение для архивации 7zip выполняет шифрование алгоритмом AES и делает все необходимые приготовления данных перед шифрованием (создание ключа-пароля, добавление сообщения к длине блока путем проверки правильности расшифровки с помощью расширенной последовательности, создание вектора инициализации и т.д.). Также было изучено, что из-за того, что размер блока AES в 2 раза больше размера блока ГОСТ 28147-89, использование ГОСТ 28147-89 также несколько увеличивает скорость шифрования на единицу.

Причина того, что шифрования диска недостаточно для обеспечения конфиденциальности данных, заключается в том, что шифрование всей цепочки инициализации с помощью UEFI Secure Boot и GPG

позволило добиться хорошего уровня защиты от замены всей системы и взлома системных программ.

Для доступа к криптографическому модулю был разработан очень удобный графический интерфейс, так что пользователь может получить доступ к командной строке и получить доступ к программе p7zip без необходимости запоминать последовательность команд.

В максимальном режиме скорость архивации можно увеличить до 2-3 раз за счет уменьшения параметров файла, и эти тесты доказали, что специально созданную архивацию, а также программу шифрования по местному стандарту можно использовать практически на любых компьютер.

Заключение. Созданный криптографический модуль протестирован и одобрен на соответствие местному стандарту. Определена эффективность работы средств защиты и изучено влияние операционной системы на загрузку вычислительных ресурсов, при этом дополнительная загрузка процессора в режиме запуска приложений не превышала 23%, а в обычном режиме работы программы не превышала превышать 17%. Адекватность полученных результатов подтверждалась статистической обработкой эксперимента.

Список литературы:

1. R. Nivedhaa, J. Jean Justus, A Secure Erasure Cloud Storage System Using Advanced Encryption Standard Algorithm and Proxy Re-Encryption – Proceedings of the 2018 IEEE International Conference on Communication and Signal Processing, ICCSP 2018.
2. Shivarajkumar Hiremath, Sanjeev R. Kunte, Ensuring Cloud Data Security using Public Auditing with Privacy Preserving – Proceedings of the 3rd International Conference on Communication and Electronics Systems, ICCES 2018.
3. Fitzroy D. Nembhard, Marco M. Carvalho, Thomas C. Eskridge, Towards the application of recommender systems to secure coding – Eurasip Journal on Information Security 2019.
4. Timo, Speedtest and Comparsion of Open-Source Cryptography Libraries and Compiler Flags, – 20.08.2022. Режим доступа:https://idlebox.net/2008/0714-cryptographyspeedtest-comparison.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ОБРАЗОВАНИИ

Рахимова Камолахон Масуджон кизи
ведущий специалист
отдела информационных коммуникаций и технологий,
Государственный центр тестирования
при Кабинете Министров,
Республики Узбекистан, г. Ташкент

Хайитов Оролбек Соатмуминович
главный специалист
отдела информационных коммуникаций и технологий,
Государственный центр тестирования
при Кабинете Министров,
Республики Узбекистан, г. Ташкент

ARTIFICIAL INTELLIGENCE IN EDUCATION

Kamolakhon Rakhimova
Leading Specialist
of the Department of Information
Communications and Technologies,
State Testing Center under the Cabinet of Ministers,
Republic of Uzbekistan, Tashkent

Orolbek Hayitov
Chief specialist
of the department of information
communications and technologies,
State Testing Center under the Cabinet of Ministers,
Republic of Uzbekistan, Tashkent

Аннотация. В статье представлена информация о развитии искусственного интеллекта во всем мире, его применении в различных областях, видах и механизмах работы, а также повышении качества образования за счет его использования в образовательном процессе. В целях обеспечения реализации Постановления Президента Республики Узбекистан от 17 февраля 2021 года №ПП-4996 «О мерах по созданию условий для ускоренного внедрения технологий искусственного интеллекта» Приводится краткий обзор информации системы, разрабо-

танные с использованием интеллекта. Несмотря на ряд недостатков искусственного интеллекта, отмечается, что при его безупречной реализации на практике можно добиться определенных преимуществ в каждой области.

Abstract. The article provides information on the development of artificial intelligence around the world, its application in various fields, types and mechanisms of operation, as well as improving the quality of education through its use in the educational process. In order to ensure the implementation of the Resolution of the President of the Republic of Uzbekistan dated February 17, 2021, No. PP-4996 "On measures to create conditions for the accelerated introduction of artificial intelligence technologies" There is a brief overview of information systems developed using intelligence. Despite a number of shortcomings of artificial intelligence, it is noted that if it is perfectly implemented in practice, it is possible to achieve some advantages in each area.

Ключевые слова: искусственный интеллект; системы; образование; программное обеспечение для прокторинга искусственного интеллекта; система онлайн-тестирования.

Keywords: artificial intelligence; systems; education; proctoring artificial intelligence software; online testing system.

Введение. Сегодня искусственный интеллект стал одной из самых важных технологий в мире. Многие сцены которые мы видели только в кино и различных фантастических романах, становятся реальностью с внедрением в нашу жизнь искусственного интеллекта. По данным ООН к 2024 году ожидается, что почти четверть мирового ВВП будет зависеть от цифровых технологий и исходя из этого лучше всего сосредоточиться на ускорении и развитии работ в этой сфере. На сегодняшний день такие страны, как Канада, Сингапур, ОАЭ, Финляндия, Япония, Китай, Италия, Тунис, Великобритания, США, Швеция, Мексика, Евросоюз, Кения, Дания, Франция, Австралия, Республика Корея, Индия и Германия объявили о стратегиях развития искусственного интеллекта.

Джон Маккарти, автор термина «искусственный интеллект», дал несколько определений искусственного интеллекта. Он описал искусственный интеллект как «науку и разработку человекоподобных интеллектуальных машин». Соответственно, компьютер можно охарактеризовать как искусственный интеллект, если он демонстрирует человеческое поведение. По словам Нильса Нильссона, другого великого ученого, автора исследований по искусственному интеллекту и многочисленных

научных публикаций в этой области, «искусственный интеллект – это теория, призванная создать имитацию естественного интеллекта». Его также можно описать как последовательность алгоритмов имитирующих человеческий разум. Из вышесказанного видно, что исследования искусственного интеллекта показали, что все во Вселенной работает в рамках определенного алгоритма [2].

Если ориентироваться на мировое образование в сфере работы в этой сфере, то, по данным Минобразования России, с 2022 года в школах проводят апробацию учебного модуля «Искусственный интеллект». Уроки искусственного интеллекта будут введены в корейских государственных школах с 2023 года. Когда темы будут включены в школьную программу в следующем году, учащиеся 2-го и 3-го классов средней школы смогут пройти курс искусственного интеллекта или уроки математики искусственного интеллекта [3]. Китай и США являются лидерами исследований и образования в области искусственного интеллекта. Помимо размещения в этих странах ведущих мировых университетов и научно-исследовательских институтов, государства полностью урегулировали механизмы поддержки инноваций и оказывают существенную финансовую поддержку институтам. В результате Китай и США привлекают все больше и больше образованных специалистов со всего мира.

Основная часть. Как отмечается в Послании Президента Республики Узбекистан Шавката Мирзиёева Олий Мажлису, в Узбекистане в развитии науки достигнуты большие успехи, и в социально-экономической сфере можно добиться больших результатов за счет использования цифровых технологий во всех областях. Развитие цифровой экономики является одним из важнейших и приоритетных направлений для Узбекистана на ближайшие годы. В соответствии со Стратегией «Цифровой Узбекистан – 2030» и быстрым внедрением технологий искусственного интеллекта и их широким использованием в нашей стране, обеспечением доступа к цифровым данным и их высоким качеством, созданы благоприятные условия для подготовки квалифицированных кадров в этой сфере [1]. Как подтверждение вышеуказанного можно рассмотреть Постановление № ПП-4996 Президента Республики Узбекистан принято от 17 февраля 2021 года «О мерах по созданию условий для ускоренного внедрения технологий искусственного интеллекта». Постановление направлено на разработку нормативной базы, определяющей единые требования, ответственность, безопасность и прозрачность при разработке и использовании технологий искусственного интеллекта в экономике и социальной сфере страны, в государственном управлении [4]. На основе с Постановлением Госу-

дарственный центр тестирования при Кабинете Министров Республики Узбекистан разработал систему прокторинга с целью внедрения первых систем искусственного интеллекта в системе образования Республики Узбекистан. Следует отметить, что программа Proctoring, основанная на системах искусственного интеллекта, имеет ряд преимуществ в контроле экзаменационного процесса.

Дистанционный контроль заявителя. Искусственный интеллект может предложить несколько способов сделать это. Хотя он не может полностью заменить человеческий контроль, он может быть ближе по качеству. Программное обеспечение Proctoring на основе систем искусственного интеллекта имеет возможность распознавания дополнительных звуков и чужих голосов (рис. 1), а также гарантирует что испытуемые не используют дополнительные инструменты и сосредотачивается на всем тестовом задании, не отвлекаясь на внешние факторы**.**

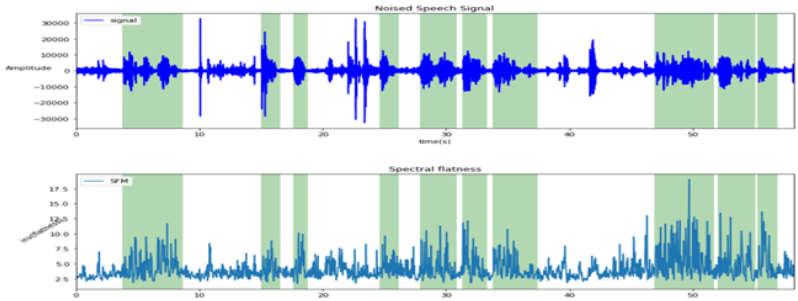


Рисунок 1. Распознавание дополнительных звуков

В результате экзамены проводятся точно, эффективно, прозрачно и справедливо. Программное обеспечение Proctoring также имеет некоторые преимущества для супервайзеров. Например, один супервайзер может одновременно дистанционно наблюдать нарушения нескольких кандидатов. При обнаружении нарушения правил экзамена супервайзер посылает онлайн-оповещения (рис. 2). Одним из важнейших преимуществ является то, что все действия, нарушения кандидатов отслеживаются и фиксируются компьютером и сохраняются в базе данных. При возникновение неопределенных ситуаций сохраненные данные позволяют уяснить возникшие вопросы.

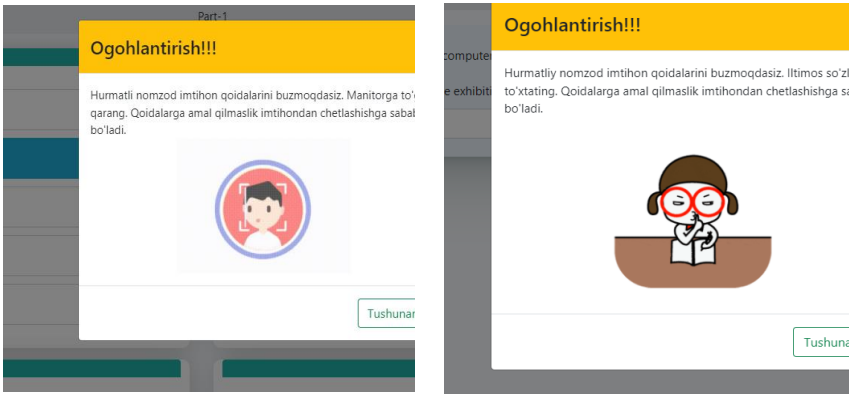


Рисунок 2. Дистанционное предупреждение о недостатках, обнаруженных искусственным интеллектом

В настоящее время Государственный центр тестирования работает над созданием еще одной «Системы онлайн-тестирования». Разрабатывается программа для биометрической идентификации с использованием системы искусственного интеллекта (рис. 3).

Рисунок 3. Распознавание человеческих лиц с помощью искусственного интеллекта

Внедрение систем с искусственным интеллектом в образование позволит оптимизировать и автоматизировать большую часть работы. Это облегчит пользователям работу над своими знаниями и повысит качество образования. Многие ученые обсуждают будущее искусственного интеллекта. Дело в том, что пока одни опасаются что они технологии могут вторгаться в частную жизнь людей и даже быть

опасными, другие ученые относятся к этому положительно утверждая, что самоуправляемые машины в системах можно использовать наиболее выгодно, с наименьшим риском и наименьшими потерями.

Вывод. Искусственный интеллект продолжает трансформировать образование в виде следующих процессов:

- В процессе глобализации и научно-технического прогресса возрастает значение искусственного интеллекта в системе образования;
- С помощью систем тестирования с использованием искусственного интеллекта экзамены проводятся точно, эффективно, прозрачно и справедливо;
- Развитие и совершенствование дистанционного обучения.

Возможности технологий искусственного интеллекта безграничны. Системы предназначены для выполнения одной конкретной задачи далеки от многозадачности. То качество технологий искусственного интеллекта, которое мы видим на экранах телевизоров и кино, день за днем входит в нашу жизнь. Разумное и умелое их использование приведет к дальнейшему развитию каждой сферы нашего существования, а также к созданию больших удобств для людей.

Список литературы:

1. Ахмедов. Б.А., Хасанова. СК (2020). Дистанционные методы обучения в повышении квалификации работников системы народного образования. Журнал инноваций в инженерных исследованиях и технологиях. Стр. 252-256.
2. Мухамедов Г'.И. и Ахмедов Б.А. (2020). Инновации кластерных мобильных приложений. Журнал академических исследований в области педагогических наук, Стр. 140-145.
3. Ахмедов. Б.А. (2020). О развитии навыков интерактивного онлайн-курса на периферии современного общества (модельная программа для педагогов общеобразовательных учреждений). Универсум: Технические науки, Стр. 11-14.
4. Постановление Президента Республики Узбекистан №ПП-4996 от 17 февраля 2021 года «О мерах по созданию условий для ускоренного внедрения технологий искусственного интеллекта».

СОВЕРШЕНСТВОВАНИЕ МЕТОДОВ ОБНАРУЖЕНИЯ ИНСАЙДЕРОВ ПОСРЕДСТВОМ ВЕРОЯТНОСТНОГО МОДЕЛИРОВАНИЯ ПОВЕДЕНИЯ НАРУШИТЕЛЯ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Стрижков Владислав Александрович
аспирант,
Федеральное государственное образовательное бюджетное учреждение высшего образования Финансовый университет при Правительстве Российской Федерации, Финансовый университет, РФ, г. Москва

Аннотация. Инсайдерские угрозы – это злонамеренные действия, мошенничество и саботаж в лице пользователей, которые прошли аутентификацию в системе легальным путём. Такие действия, как правило, совершаются в отношении информации об интеллектуальной собственности или безопасности. Несмотря на то, то количество внутренних угроз намного меньше, чем атак со стороны внешних хакеров, инсайдеры могут нанести значительный ущерб. Поскольку инсайдеры знакомы с организационной системой, очень сложно определить их вредное поведение. Консервативные пути выявления внутренних угроз направлены на длительное и трудоёмкое поисковое действие, поэтому они не являются достаточно эффективными и не всегда безошибочны. В данной статье предлагается методика изобличения инсайдеров, работающая за счёт алгоритмов вычисления аномалий и моделирования наиболее вероятного поведения пользователей в охраняемом информационном пространстве. Анализируя системные логи из источников данных о действиях пользователя можно запротоколировать сведения об их действиях и составить картину нормального поведения. Такие сведения можно черпать, к примеру, из содержимого электронной почты, журналов событий на рабочих станциях пользователей, временных промежутках активности пользователей и т. д. После этого, на основании полученных данный создаётся алгоритм, выявляющий подозрительное и некорректное поведение пользователя, обращение им к информации, являющейся избыточной для выполнения его служебных обязанностей и выходящей за рамки его компетенций. Тем самым алгоритм подмечает вероятное направление реализации в последующем вредоносных действий. Таким образом, возникает иной способ изобличения инсайдера, основная его положительная черта в сравнении с другими подходами в независимости от свойств случайных процессов,

характеризующих работу пользователя. Кроме того, данный подход снижает вероятности ошибок первого и второго рода, то есть на выходе получится куда меньшее количество как ложных срабатываний, так и упущенных, но реально присутствующих угроз безопасности. Для исключения ложных срабатываний предложенный метод в том числе опирается на теорию запретов, в рамках которой задана вероятностная величина, описывающая действия пользователя, не содержащих злого умысла. За счёт этого обосновывается точность построенного алгоритма обнаружения реальных внутренних угроз в большом массиве пользователей. В методе создаётся новое программное средство, моделирующее деятельность честных пользователей и инсайдеров в системе в виде имитации. Такое ПО помогает оценить границы реальной применимости консервативных методов математической статистики в новом подходе, основанном на имитационном моделировании. Неразрывно с математической статистикой в исследовании также применяются все применимые в данной ситуации методы теории вероятностей и теории множеств. При изучении теоретической части исследуемой области был проведен научный анализ имеющихся результатов в применении теории запретов и современных методик распознавания инсайдеров. При подтверждении практической эффективности предлагаемого метода произведено имитационное моделирование. Создаваемый подход даёт возможность проводить анализ инцидентов информационной безопасности, связанных с любыми вероятностными событиями, как несанкционированные действиями пользователей, так и любые другие. Этот метод может применяться и для улучшения ныне уже существующих систем обнаружения внутренних нарушителей, и в качестве нового независимого метода обнаружения несанкционированного сбора информации работниками.

Ключевые слова: инсайдер; моделирование поведения; внутренний нарушитель; теория статистики; информационная безопасность; инсайдерская угроза; вероятностная модель; алгоритм обнаружения аномалий.

1. Введение

Инсайдерская угроза – это угроза безопасности, определяемая тем, что в числе доверенных лиц внутри охраняемой сети присутствует злоумышленник [1]. Несмотря на то, что угрозы внутреннего характера случаются не часто, размер их ущерба превышает потери от внешних атак [2,3]. Инсайдеры располагают всей необходимой информаци-

ей о компьютерной сети своей организации и имеют легальный доступ ко всем операционным процессам. Иногда не удаётся своевременно определить, когда их действия носят злонамеренный характер [4]. Был создан ряд системных технологий защиты от вторжения извне, таких как количественная оценка интернет-протокола подключения (IP) и разновидности атаки [5]. Всё это в целом указывает на то, что в направлении информационной безопасности приоритет отдаётся защите от внешних нарушителей, а поиск внутренних угроз получает недостаточно внимания и ресурсов [6].

Имеется три ключевых стратегии исследования для выявления внутренних угроз. Первая стратегия при построении системы обнаружения опирается на правила и сценарии [7,8]. Для этого экспертной группой создаются сценарии злонамеренных действий внутренних нарушителей. В последующем поведение всех пользователей фиксируется в форме журнала действий и регулярно проверяется на предмет соответствия ранее описанным сценариям. Такой способ выявления инсайдеров имеет существенный недостаток, состоящий в необходимости непрерывной доработки и написании новых сценариев экспертными группами в данной отрасли, иначе, при их устаревании, сразу возникает риск обойти их [9]. Таким образом, метод, основанный на сценариях, не обеспечивает должного уровня защищенности от внутренних угроз [7,10,11]. Вторая стратегия основана на создании сетевого интерфейса для обнаружения подозрительного или нежелательного поведения посредством мониторинга изменений в графической структуре [12]. Помимо того, что этот метод определяет не только аналитическую ценность самих сведений, но он так же устанавливает взаимосвязь между ними. Взаимосвязи представлены в виде рёбер, связывающих узлы графика. Свойства графиков можно подвергнуть аналитической проверке для установления связей между конкретными узлами и внутренними угрозами. Таким образом, патологические действия позволяют определить, когда модификации, добавление или стирание достигают базовой структуры графика данных. Третья стратегия основана на создании статистической модели обучения, учитывающей сведения о прошлом для прогнозирования потенциально опасного поведения [14]. Машинное обучение – это методика, при которой машина обучается алгоритму оптимизации критериев производительности в соответствии с данными обучения для исполнения необходимых задач [15]. Внутреннее обнаружение угроз в машинном обучении предназначено для создания механизма автоматического вычисления пользователей, совершающих нормальные действия, из общего числа работников, не имея никаких заранее прописанных правил. Концепция машинного обучения опирается на принцип постоян-

ного обучения и доработки алгоритмов с использованием больших данных. Такой подход обеспечивает более надежное выявление внутренних нарушителей в сравнении с составленными экспертами вручную сценариями. Методология машинного обучения способна формировать возможные сценарии внутреннего нарушителя, вызывающие несанкционированные действия, анализируя высокоуровневые статистические модели. В этих целях определяются переменные, которые представляют собой различные действия внутреннего нарушителя как, например, электронные письма, файлы и подключение, в последующем используются статистические показатели и всевозможные алгоритмы машинного обучения для выбора самого подходящего сценария поведения. Например, можно определить инсайдера, анализируя сходство поведения между ролью Группы, в которую пользователь фактически входит, и другой ролью Группы, к которой он не относится, полагая, что пользователи в одних и тех же группах ролей обладают аналогичными моделями поведения. Так как поведение пользователя можно получить из разнообразных источников информации, например, из системных журналов, отправленной и полученной электронной почты, из вложений электронной почты, в таком случае основным моментом в создании эффективной модели обнаружения инсайдеров является выявление полезных функций для всяческих типов данных и преобразование неструктурированных исходных данных в упорядоченную последовательность.

Для устранения минусов всех трёх вышеизложенных подходов к идентификации внутренних нарушителей предлагается новый подход выявления инсайдеров, основанный на имитационном моделировании поведения пользователя. На старте, в ходе моделирования действий пользователя во внимание берутся три типа сведений. Во-первых, перечень журналов активности физического лица, зарегистрированных в системе. В случае, если системные журналы включают сведения о том, что пользователь подключает к машине съёмный USB-накопитель, то суммарное количество подключений каждый день можно найти в качестве переменной. Во-вторых, изучается создаваемый пользователем контент, такой как, к примеру, содержимое писем электронной почты. В-третьих, выстраивается сеть общения с пользователями на основе электронной почты, обмена файлами. После этого для узла вычисляются сводные статистические данные, в дальнейшем они помогают определении поведенческих признаков. При построении модели обнаружения угроз учитываются извлеченные и накопленные на основе трех категорий данные для изучения характеристик обычной деятельности.

2. Набор данных и моделирование поведения пользователей

Поведение пользователя хранится в базе данных в виде соответствующих таблиц: авторизация в системе, использование USB-носителей, скачанные файлы и т. д. Для мультифакторного анализа поведения пользователей следует систематизировать накопленные данные, поэтому информацию о поведении необходимо располагать в хронологическом порядке, а также упорядочивать на регулярной основе. Рассматривая фрагментированную активность пользователя на ежедневной основе и складывая её, мы получаем входную переменную модели выявления угроз, описывающую интенсивность деятельности. Для нахождения входных переменных для выявления угроз, применяются входные сведения подобные тем, что представлены таблицах 1 и 2. Поэтому, сводная информация о поведении за конкретный день, собранная для каждого пользователя системы, сравнивается с нормальным поведением. Модель, представленная в таблицах, и значения аномалий – это лишь малая часть, характеризующая имитацию инсайдерского поведения, в которой его можно идентифицировать. Чаще всего нестандартное поведение (почти 90%) фиксируется со стороны трёх ролевых лиц: "Продавец", "ИТ-администратор", "Инженер-электрик". Поэтому для них существует больший запас для записи приемлемого числа аномалий. В ином случае, когда аномальные данные поступают от разработчиков или программистов. В этом случае система сразу же сосредотачивается на поиске возможных внутренних угроз.

Таблица 1.

Количество допустимых аномальных записей в соответствии с ролью

Роль	Количество допустимых аномальных записей
Продавец	32
ИТ-администратор	23
Инженер-электрик	10
Компьютерный программист	3
Менеджер	2
Директор	1
Рабочий производственной линии	1
Разработчик ПО	1
Всего	73

Таблица 2.

Частота записей трех ролей

Инженер-электрик		ИТ-администратор		Продавец	
Нормальная	**Аномальная**	**Нормальная**	**Аномальная**	**Нормальная**	**Аномальная**
141,199	10	34,244	23	125,524	32

В табл. 3 приведены данные для выявления внутреннего нарушителя на основе анализа содержимого электронной почты. Столбцы “Тема 1” – “Тема 50” показывают вероятности, назначенные по 50 темам на индивидуальное электронное письмо и используются в качестве входной переменной модели обнаружения аномалий. Сумма вероятностей 50 тем всегда равна 1. “Идентификатор” – это уникальный номер строки для разных наблюдений. “Цель” – это переменная, указывающая на то, является ли электронное письмо аномальным (1) или нормальным (0). В табл. 4 показано количество аномальных и нормальных электронных писем для каждой из трёх ролей. Предполагается, что распределение тем почты для каждой роли осуществляется подобным образом. Так, если распределение определенного электронного письма значительно разнится с другими электронными письмами, то это является основанием подозревать присутствие вредоносных действий.

Таблица 3.

Количественные примеры содержимого электронной почты

Идентификатор	Тема 1	Тема 2	…	Тема 50	Цель
(I1O2-B4EB49RW-7379WSQW)	0.008	0.012	…	0.154	1
(L7E7-V4UX89RR-3036ZDHU)	0.021	0.008	…	0.125	1
(S8C2-Q8YX87DJ-0516SIWZ)	0.014	0.006	…	0.145	0
(A1V9-O5BL46SW-1708NAEC)	0.352	0.014	…	0.086	0
(N6R0-M2EI82DM-5583LSUM)	0.412	0.058	…	0.285	0
(O2N1-C4ZZ85NQ-8332GEGR)	0.085	0.421	…	0.001	0

Таблица 4.

Нормальное и аномальное количество электронных писем для трех ролей

Инженер-электрик		ИТ-администратор		Продавец	
Нормальное	Аномальное	Нормальное	Аномальное	Нормальное	Аномальное
644,252	40	170,765	15	694,050	13

Так как сведения об отправителе/получателе можно также получить из записей журнала электронной почты, в дальнейшем можно на регулярной основе строить граф в виде связей пользователей по электронной почте и извлекать количественные характеристики в качестве третьего источника анализа активности пользователей для выявления инсайдерской угрозы.

3. Обнаружение инсайдерской угрозы

На рисунке 1 отображена общая структура метода обнаружения внутренних угроз. На стадии моделирования поведение пользователя, хранящееся в системе каждого журнала, преобразуется в три типа наборов данных: сводка повседневной деятельности, содержимое электронной почты и электронная почта в качестве сети связи. На стадии обнаружения аномалий используются алгоритмы классификации одного класса на основе трёх наборов данных. Как только новая запись становится доступной, она помещается в одну из этих трех частей модели, чтобы предсказать возможные вредоносные результаты.

Рисунок. 1. Система обнаружения внутренних угроз

Для домена обнаружения внутренних угроз очень часто доступно очень большое количество случаев нормальной активности пользователя, тогда как ненормальных случаев доступно лишь несколько или совсем нет. В этом случае традиционные алгоритмы бинарной классификации не могут быть обучены из-за отсутствия аномальных классов [19]. В качестве альтернативы, в несбалансированных средах данных в отличие от бинарной классификации, классификация с одним классом использует только данные обычного класса для изучения их общих характеристик, не полагаясь на данные аномального класса [20]. Как только модель классификации одного класса обучена, она предсказывает вероятность того, что вновь заданный экземпляр будет обычным экземпляром класса. В этой статье используется анализ основных компонентов (PCA), оценка плотности Гаусса (Gauss), оценка плотности окна Парзена (Parzen) и кластеризация K-средних (KMC) в качестве алгоритмов одноклассовой классификации для выявления внутренних угроз, как показано на рисунке 2.

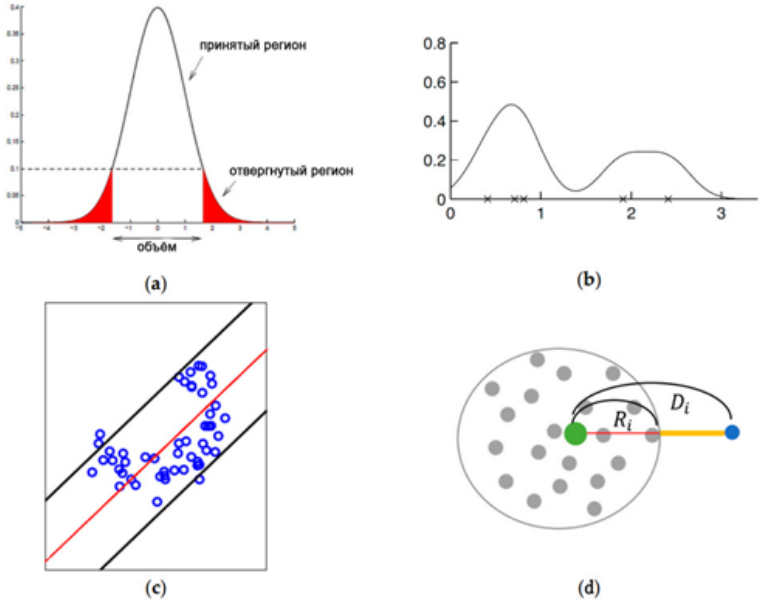


Рисунок 2. Четыре алгоритма обнаружения аномалий, используемые в этой статье: (a) оценка плотности по Гауссу, (b) оценка плотности окна Парзена, (c) анализ главных компонентов (PCA) и (d) кластеризация K-средних (KMC)

Для внутреннего обнаружения угроз, как правило, поддерживается очень большое количество обычной деятельности пользователей, однако для аномальных случаев это число крайне мало. В случае традиционных алгоритмов бинарной классификации они не могут быть изучены из-за отсутствия аномальных классов [17]. Как альтернатива, классификация по несбалансированной информации, в отличие от двоичной классификации, использует для изучения данные только от общего класса, не учитывая аномальный класс [16]. После того, как распределенная модель обучается классом, она предугадывает вероятность того, что все новые примеры. В этой статье используется оценка плотности по Гауссу (Gauss), уплотнение загрузочных окон (Parzen), анализ основных компонентов (PCA) и кластер k-среднего (KMC) используется в качестве единого алгоритма классификации для выявления внутренних угроз, как видно на рисунке 2.

Помимо индивидуального выявления аномалий алгоритмов, нас интересует и комбинация этих алгоритмов. Даже при изучении одних и тех же данных методология создания оптимальной модели для каждого алгоритма различна, поэтому нет единого алгоритма, который лучше во всех ситуациях [16]. Итак, мы рассмотрели все возможные комбинации четырех отдельных детекторов аномалий с целью определить оптимальную комбинацию набора данных.

4. Результаты

Обычно алгоритм вычисления аномалий обучается только на основе обычных данных в ситуациях, когда большая часть случаев находится в нормальном классе, а только несколько экземпляров в ненормальном классе. При таком раскладе проблематично установить порог обнаружения. Качественные свойства обнаружителей аномалий оцениваются в следующем порядке. Сначала информация разбивается на набор данных, содержащий 90% выбранных произвольно нормальных экземпляров, и ещё на 10% тестовых данных, который содержит остаточные нормальные экземпляры, а также полный перечень ненормальных экземпляров. Затем алгоритм обнаружения обучается только на базе обучающих данных. В итоге вычисляется истинная вероятность выявления в соответствии с семью значениями порога (1%, 5%, 10%, 15%, 20%, 25% и 30%) по уравнению:

$$\text{Истинная частота обнаружения (в верхнем X\%)} = \frac{\text{Количество вредоносных действий,включенных в верхние оценки аномалий X\%}}{\text{Общее количество вредоносных действий}} \quad (1)$$

Чтобы получить статистически допустимые результаты, данный алгоритм воспроизводится 30 раз. Для каждого алгоритма обнаруже-

ния аномалий средний истинный коэффициент обнаружения в верхнем X% применяется в качестве показателя действенности выявления внутреннего нарушителя.

В таблицах 5-7 показана эффективность охвата внутренних нарушителей лучшей из выбранных комбинаций (например, «Parsen + PCA»), на основе данных о ежедневной активности для трех ролей: «ИТ-администратор», «Продавец» и «Инженер-электрик». Как объяснялось ранее, мы протестировали все комбинации нескольких моделей «Parsen + PCA», так что это привело к лучшей совместимости в 10 случаях из 21, за которыми последовал «Gauss + Parsen + PCA» (5 случаев). Так в числе первых 1% оценок аномалий с наивысшим рейтингом, предугаданных Gauss для «Инженер-электрик», с легкостью выявляется половина вредоносных действий, что уже в 50 больше, чем способна распознать случайная модель, которая в конечном итоге обнаруживает лишь 1% ненормального поведения.

Таблица 5.

Истинная вероятность обнаружения аномалий для каждого алгоритма на основе анализа повседневных действий, сводка для «Инженер-электрик» (наилучший результат – жирным шрифтом)

Ранг аномалии	Gauss	Parsen	PCA	КМС (К = 3)	КМС (К = 5)	КМС (К = 10)	Parsen + PCA
1%	0.5000	0.4000	0.4933	0.5233	0.5333	**0.5367**	0.4833
5%	0.6000	0.5000	0.6667	0.6400	0.6300	0.6333	**0.7633**
10%	0.6167	**0.7933**	0.7467	0.7033	0.6467	0.6933	**0.7933**
15%	0.7000	**0.9000**	0.7800	0.7167	0.6767	0.7333	0.8000
20%	0.7000	**0.9000**	0.7900	0.7500	0.6967	0.7600	0.8167
25%	0.7000	**0.9000**	0.8000	0.7767	0.7433	0.7767	0.8233
30%	0.7000	**0.9000**	0.8033	0.7677	0.7700	0.7933	0.8500

Таблица 6.

Истинная вероятность обнаружения аномалий для каждого алгоритма на основе анализа повседневных действий, сводка для «ИТ-администратор» (наилучший результат – жирным шрифтом)

Ранг аномалии	Gauss	Parsen	PCA	КМС (К = 3)	КМС (К = 5)	КМС (К = 10)	Parsen + PCA
1%	0.0435	0.0478	0.0739	0.0580	0.0521	0.0522	**0.0971**
5%	0.0435	0.1739	0.2130	0.0841	0.0739	0.0768	**0.2174**
10%	0.0435	**0.3015**	0.2304	0.1246	0.1087	0.1174	0.2580

Ранг аномалии	Gauss	Parsen	PCA	КМС (К = 3)	КМС (К = 5)	КМС (К = 10)	Parsen + PCA
15%	0.0971	**0.3043**	0.2884	0.1391	0.1275	0.1362	0.2913
20%	0.1594	0.3043	**0.3348**	0.2333	0.2000	0.2043	0.3246
25%	0.1739	0.3043	**0.3681**	0.3029	0.2681	0.2797	0.3551
30%	0.2609	0.3043	**0.4087**	0.3493	0.3304	0.3406	0.3928

Для роли «Инженер-электрик», где 1% наиболее вероятного аномального поведения контролируется ежедневно, система способна обнаружить не более 53,66% фактических конфиденциальных данных. Эти показатели возрастают до 76,33%, 79,33% и 90%, при этом процент наблюдаемых аномального поведения возрастает до 5%, 10% и 15% соответственно. Для роли "ИТ-администратор" выявление не настолько вероятно, как у «Инженер-электрик», но тем не менее ощутимо лучше, чем случайная модель. Увеличение истинной вероятности выявления в сравнении со случайным предположением – 9,71%, отсечка 1% или 21,74%.

Таблица 7.

Истинная вероятность обнаружения аномалий для каждого алгоритма обнаружения на основе анализа повседневных действий, сводка для «Продавец» (наилучший результат – жирным шрифтом)

Ранг аномалии	Gauss	Parsen	PCA	КМС (К = 3)	КМС (К = 5)	КМС (К = 10)	Parsen + PCA
1%	0.0093	**0.1177**	0.0781	0.0375	0.0396	0.0281	0.1021
5%	0.0313	0.3217	0.3375	0.1083	0.0843	0.0802	**0.3406**
10%	0.0313	0.5677	0.5458	0.1396	0.1125	0.1135	**0.6156**
15%	0.6563	0.5844	0.6625	0.2604	0.1969	0.2115	**0.7958**
20%	0.6563	0.7781	0.7177	0.2938	0.2427	0.2416	**0.8646**
25%	0.6563	0.8396	0.7677	0.3240	0.2854	0.2802	**0.9041**
30%	0.6563	0.8719	0.8042	0.3927	0.3260	0.3219	**0.9479**

Среди всех алгоритмов Parsen показал самые высокие показатели обнаружения в 8 случаях из 21. Обратите также внимание на то, что комбинация «Parsen + PCA» в ряде случаев обеспечивает высочайшую результативность обнаружения.

5. Заключение

В этой статье предложен метод обнаружения внутренних угроз на основе поведения пользователя, с применением алгоритмов моделирования и обнаружения аномалий. При моделировании поведения поль-

зователей разнородное поведение преобразуется в структурированный набор данных (день пользователя, содержимое электронной почты, неделя пользователя), где каждый столбец связан с входными переменными для моделей обнаружения аномалий. Построено два набора данных, а именно набор сводных данных об активности на основе журналов активности пользователей и набор данных содержимого электронной почты на основе темы моделирования. На основе этих наборов данных продемонстрирована система обнаружения внутренних угроз с использованием имитационного моделирования и алгоритмов обнаружения аномалий для имитации реального поведения инсайдеров, которые ведут себя потенциально злонамеренно. Экспериментальные результаты показывают, что предложенная структура может достаточно хорошо работать для обнаружения инсайдеров. На основе ежедневной активности обнаружение аномалий обеспечило 53,67 % вероятность обнаружения инсайдера, отслеживая при этом только 1 % подозрительных действий. Когда охват подозрительных действий был расширен до 30%, то уже более 90% фактического аномального поведения были обнаружены для двух ролей из трех оцениваемых. Хотя предложенная схема была проверена эмпирически, в ней есть некоторые ограничения. Предложенная модель обнаружения внутренних угроз работает на основе конкретных единиц времени, например, сутки. Другими словами, этот подход может обнаруживать злонамеренное поведение на основе продолжительного времени, но не может обнаружить их в режиме реального времени. Следовательно, возможно, стоит разработать модель обнаружения внутренних угроз на основе последовательности, которая способна обрабатывать данные онлайн-потока.

Список литературы:

1. Sharma B., Pokharel P., Joshi B. User Behavior Analytics for Anomaly Detection Using LSTM Autoencoder – Insider Threat Detection; Bangkok, Thailand. 1–3 July 2020; New York, NY, USA: Association for Computing Machinery (ACM); 2020. pp. 1–9.
2. Lee C., Iesiev A., Usher M., Harz D., McMillen D. IBM X-Force Threat Intelligence Index. 2020. Available online: https://www.ibm.com/security/data-breach/threat-intelligence.
3. Erdin E., Aksu H., Uluagac S., Vai M., Akkaya K. OS Independent and Hardware-Assisted Insider Threat Detection and Prevention Framework; Proceedings of the 2018 IEEE Military Communications Conference (MILCOM2018); Los Angeles, CA, USA. 29–31 October 2018; pp. 926–932.
4. Almehmadi A. Micromovement Behavior as an Intention Detection Measurement for Preventing Insider Threats. IEEE Access. 2018; 6:40626–40637. doi: 10.1109/ACCESS.2018.2857450.

5. Kim J., Park M., Cho S., Kang P. Insider Threat Detection Based on User Behavior Modeling and Anomaly Detection Algorithms. Appl. Sci. 2019; 9:4018. doi: 10.3390/app9194018
6. Alpaydin E. Introduction to Machine Learning. MIT Press; Cambridge, MA, USA: 2020.
7. Homoliak I., Toffalini F., Guarnizo J., Elovici Y., Ochoa M. Insight into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. ACM Comput. Surv. 2018; 52:30. doi: 10.1145/3303771.
8. Yuan S., Wu X. Deep learning for insider threat detection: Review, challenges and opportunities. Comput. Secur. 2021; 104:102221. doi: 10.1016/j.cose.2021.102221.
9. Kim A., Oh J., Ryu J., Lee K. A Review of Insider Threat Detection Approaches with IoT Perspective. IEEE Access. 2020; 8:78847–78867. doi: 10.1109/ACCESS.2020.2990195.
10. Al-Mhiqani M., Ahmad R., Abidin Z., Yassin W., Hassan A., Abdulkareem K., Ali N., Yunos Z. A Review of Insider Threat Detection. Appl. Sci. 2020; 10:5208. doi: 10.3390/app10155208.
11. Alsowail R., Al-Shehari T. A Multi-Tiered Framework for Insider Threat Prevention. Electronics. 2021; 10:1005. doi: 10.3390/electronics10091005.
12. Georgiadou A., Mouzakitis S., Askounis D. Detecting Insider Threat via a Cyber-Security Culture Framework.J. Comput. Inf. Syst. 2021:1–11. doi: 10.1080/08874417.2021.1903367.
13. Alhajjar E., Bradley T. Survival analysis for insider threat. Comput. Math. Organ. Theory. 2021:1–17. doi: 10.1007/s10588-021-09341-0.
14. Denney K., Babun L., Uluagac A.S. USB-Watch: A Generalized Hardware-Assisted Insider Threat Detection Framework.J. Hardw. Syst. Secur. 2020; 4:136–149. doi: 10.1007/s41635-020-00092-z.
15. Le D.C., Khanchi S., Zincir-Heywood A.N., Heywood M.I., Le D.C. Benchmarking evolutionary computation approaches to insider threat detection; Kyoto, Japan. 15–19 July 2018; pp. 1286–1293.
16. Tian Z., Shi W., Tan Z., Qiu J., Sun Y., Jiang F., Liu Y. Deep Learning and Dempster-Shafer Theory Based Insider Threat Detection. Mob. Netw. Appl. 2020:1–10. doi: 10.1007/s11036-020-01656-7.
17. Sav U., Magar G. Inventive Computation and Information Technologies. Springer; Berlin/Heidelberg, Germany: 2020. Insider Threat Detection Based on Anomalous Behavior of User for Cybersecurity; pp. 17–28.

1.2. ЭНЕРГЕТИКА

CIM-МОДЕЛЬ. СОЗДАНИЕ ЕДИНОЙ ЦИФРОВОЙ МОДЕЛИ

Литовка Мария Алексеевна
студент,
Государственный университет аэрокосмического приборостроения,
РФ, Санкт-Петербург

Проблема информационной совместимости и интеграции систем – одна из ключевых, с которыми сталкиваются руководители ИТ-направлений компаний при реализации стратегии цифровой трансформации. Наличие большого количества систем различных производителей с закрытыми внутренними моделями баз данных зачастую ставят под сомнение реализуемость и экономическую целесообразность такой интеграции. Хранение, каталогизация и использование данных в универсальном формате в соответствии со стандартом CIM позволят создать единое информационное пространство электроэнергетических систем и решить вопросы интеграции ПТК с различными корпоративными информационными системами предприятий.

CIM – это набор открытых стандартов, разработанных Международной Электротехнической Комиссией (англ. IEC) для описания электроэнергетических систем. CIM был задуман для того, чтобы дать общепонятные определения элементов электроэнергетических систем, их свойств и связей между ними для использования в системах управления производством и передачей электроэнергии (EMS) и их программных интерфейсах. В настоящее время разрабатывается 57 Техническим комитетом МЭК в нескольких рабочих группах.

Состав CIM:

- Стандарт МЭК 61970 описывает базовые понятия CIM. Он одобрен большинством поставщиков EMS-решений, что позволяет обмениваться данными между их приложениями, независимо от внутренней архитектуры ПО и используемой операционной платформы.
- Стандарт МЭК 61968 расширяет модель CIM, покрывая другие аспекты обмена данными для ПО в области электроэнергетики, такие как учет основных средств, планирование работ, биллинг.

• Стандарт МЭК 62325 расширяет оба перечисленных выше стандарта в части обмена данными между участниками энергетических рынков.

Создание CIM-модели – не простой процесс. Он требует специальных усилий, как в части подготовки данных, так и в части организационных механизмов обработки данных.

Первые шаги на пути создания Единой информационной модели ЕЭС России (ЕИМ) были сделаны в 2006 году, когда применение стандартов CIM в международной практике еще набирало обороты. В 2013 году началась активная фаза создания ЕИМ. Разработка модели завершилась к 2016 году, и на работу с ней были переведены два деловых процесса из числа выполняемых Системным оператором – расчет установившихся режимов и оценка со стояния энергосистемы. Затем началось поэтапное увеличение количества информации в ЕИМ и перевод других задач на использование данных ЕИМ. Постепенно с ЕИМ были интегрированы программные комплексы для управления ремонтами, оперативно-информационный комплекс и другие информационные системы.

Вскоре стало ясно, что путь унификации программных средств Системного оператора и их взаимной интеграции путем так называемой кроссировки (через таблицы соответствия) является далек от оптимального и не решает всех проблем информационного обмена. Требовался переход к использованию единых принципов и технологий взаимодействия информационных систем, включая единые структуру данных и формат информационного обмена. К тому же в тот период на фоне реформирования отрасли с разделением по видам деятельности начал более активно развиваться информационный обмен диспетчерских центров с субъектами отрасли, что только усугубляло непростую ситуацию в области обмена данными.

С учетом того, что профиль ЕИМ будет развиваться, Системный оператор строил свою систему управления моделью таким образом, чтобы иметь возможность самостоятельно, без привлечения разработчиков добавлять новые классы, атрибуты, своими силами проводить инжиниринг данных, добавлять в модель непосредственно экземпляры объектов и данные по ним. В настоящее время каноническая модель содержит 902 класса, 2254 атрибута, 1296 связей, в ней представлено 6,6 миллиона именованных объектов.

На пути создания единой информационной модели пришло Создание Единой информационной модели ЕЭС России понимание, что помимо соответствующей внутренней стандартизации информационного обмена, нужно двигаться и к отраслевой. В решении этого вопро-

са активное участие приняло Минэнерго России. В сотрудничестве с отраслевым министерством Системный оператор инициировал разработку национальных стандартов для обеспечения перехода к стандартизированному информационному обмену, построенному на базе стандартов CIM. Было ясно, что это будет «русский CIM», дополненный особенностями, характерными исключительно для российской электроэнергетики, в частности, такими, как трехуровневая структура диспетчерского управления и масштабы ЕЭС России

Процесс создания ЕИМ можно разделить на два этапа. Изначально предполагалось, что первичный инжиниринг данных будет выполнен подрядчиком, что позволит «сгладить» процесс ее внедрения и сразу приступить к ее эксплуатации и использованию ее данных в технологических задачах. На этом этапе специалистами Системного оператора проведена большая работа по сбору сводных данных для передачи подрядчику. После создания информационной модели, которая охватывала три операционные зоны (ОДУ Северо-Запада, ОДУ Центра и ОДУ Юга), стало понятно, что проверка, верификация и актуализация далеко не полной модели очень трудозатратны, а детальная верификация модели на стороне подрядчика практически невозможна.

Второй этап создания ЕИМ включал в себя инжиниринг данных модели операционных зон ОДУ Урала, ОДУ Средней Волги, ОДУ Сибири и ОДУ Востока. На этом этапе специалисты Системного оператора сразу приступили к самостоятельному созданию модели, что позволило ускорить внедрение модели в эксплуатацию.

Несмотря на то, что первичный инжиниринг данных был выполнен на стороне подрядчика, доработка модели оказалась непростой задачей и потребовала колоссального напряжения и усилий как руководителей, так и специалистов, работающих непосредственно над созданием ЕИМ. Не всегда было легко выявить ошибки и неточности, ведь проверка расчетов осуществлялась также на вновь разработанном ПО, алгоритмы расчетов которого проходили практическую апробацию. Основная тяжесть легла на плечи специалистов технологического функционального блока АО «СО ЕЭС», которые держат информацию об объектах ЕЭС России буквально на кончиках пальцев и понимают конкретные значения тех или иных параметров, а также цену ошибки при внесении недостоверных данных. Итогом второго этапа стало создание и использование основных деловых процессов Единой информационной модели ЕЭС России. В 2016 году программный комплекс по управлению ЕИМ был отлажен и введен в работу, также был запущен процесс поддержания модели в актуальном состоянии – процесс внесения изменений и проверки корректности данных. Создание моде-

ли – это длительный, трудоемкий и тяжелый процесс, который Системному оператору все-таки удалось пройти. Нужны усилия и кропотливый труд именно тех специалистов, которые эти данные будут в дальнейшем использовать. Потому что та модель, которая не используется регулярно, быстро устаревает, а модель, которая не известна людям, вносящим в нее данные, обычно содержит большое количество ошибок. Только за счет привлечения к созданию ЕИМ специалистов, которые понимают, что с этой моделью им дальше работать, Системному оператору удалось создать качественный цифровой продукт.

Для верификации данных модели в Системном операторе была разработана серия формализованных правил проверки данных. Правила позволяют в автоматизированном режиме (при помощи специального ПО) последовательно проверить данные на совместность, наличие пустых значений, ошибки и опечатки, на превышение допустимых пределов введенной величины. Алгоритм также предусматривает проверку данных в ходе выполнения расчетных задач – расчетов установившихся режимов и оценки состояния, то есть тех режимных задач, которые стали пилотными при внедрении ЕИМ.

В настоящее время идет процесс перевода на CIM иных комплексов, эксплуатируемых Системным оператором. Поэтапный перевод основного программного обеспечения Системного оператора на работу с информационной моделью позволит достичь целевой модели, в которой существует единый источник НСИ на базе CIM-модели, а информационный обмен между приложениями происходит без многочисленных преобразований данных.

На нынешнем этапе в России первоочередными задачами являются закрепление отработанных принципов создания ЕИМ в национальных стандартах и отраслевых нормативных правовых актах, описание общеотраслевых правил моделирования на основе CIM, а также утверждение порядка создания и сопровождения информационной модели электроэнергетики, включающего правила идентификации объектов.

Список литературы:

1. Куканов А.В., Моржин Ю.И. Архитектура систем управления данными для интеллектуальной энергетики. Энергия единой сети. 2013. № 4.
2. Common Information Model в России и в мире (№1, 2021 г.) – конференция АО «СО ЕЭС»
3. Концепция «Цифровая трансформация 2030» ПАО «Россети», 21.12.2018

РАЗДЕЛ 2.

МАТЕМАТИКА

2.1. ВЫЧИСЛИТЕЛЬНАЯ МАТЕМАТИКА

ОЦЕНКА ПАРАМЕТРОВ РЕЗОНАНСОВ ЧЕРЕЗ РАЗЛОЖЕНИЕ СПЕКТРОВ ИЗЛУЧЕНИЯ ПО ГАУССОВЫМ ВЕЙВЛЕТАМ 2-ГО ПОРЯДКА

Подосенова Татьяна Борисовна
канд. физ.-мат. наук,
старший научный сотрудник,
Московский государственный университет
имени М.В. Ломоносова,
РФ, г. Москва

ESTIMATION OF RESONANCES PARAMETERS THROUGH THE DECOMPOSITION OF RADIATION SPECTRA BY USING OF GAUSSIAN WAVELETS OF THE 2ND ORDER

Tatyana Podosenova
Candidate of Science
in Physics and Mathematics, Senior Researcher,
Lomonosov Moscow State University,
Russia, Moscow

Аннотация. На основе метода непрерывного вейвлет-преобразования спектров, и с выбором гауссовых вейвлетов в качестве базисных, в работе получены аналитические выражения для оценок параметров полуширины и амплитуды резонансных линий. В формулах оценок используются вычисленные в точках центров резонансов значения отношений вейвлет-коэффициентов, полученных при разложениях спектра по двум различающимся параметрами масштаба гауссовым

вейвлетам 2-го порядка. Описанные алгоритмы реализованы на языке системы компьютерной математики Matlab.

Abstract. By using of the continuous wavelet transformation of spectra and with the Gaussian wavelets as the base ones, the analytical expressions for estimating the parameters of the half-width and amplitude of resonant lines are considered in the paper. The formulas for the estimates use the values of the ratios of the wavelet coefficients which are calculated at the points of resonances centers. These coefficients are obtained as a result of the transformation of the spectra by two different Gaussian wavelets of the 2nd order corresponding to different scale values. The described algorithms are realized for the computer mathematics Matlab system.

Ключевые слова: спектр излучения; резонансная линия; непрерывное вейвлет-преобразование; гауссов вейвлет.

Keywords: radiation spectrum; resonance line; continuous wavelet transform; Gaussian wavelet.

1. Полученные в результате аппаратурных измерений спектры излучения рассматриваются в работе в виде суммы трех компонент – полезной, гладкой базовой и шумовой составляющих:

$$y = \{y_i = Y(x_i) + B(x_i) + \varepsilon_i\,, i = 1,...,N\},\ Y(x) = \sum\nolimits_j A_j g_j(x)\,, \quad (1)$$

где $\{B(x_i)\}$ – гладкая базовая кривая, $\{\varepsilon_i\,, i = 1,...,N\}$ – шумовая компонента. В работе мы ограничимся гауссовой моделью формы резонансных линий:

$$g_j(x) = g_0(x; \mu_j, \beta_j)\,, \quad (2)$$

$$g_0(x; \mu, \beta) = e^{-(x-\mu)^2/(2\beta^2)},\ \int_{-\infty}^{\infty} g_0(x; \mu, \beta)dx = \sqrt{2\pi}\beta,\ \beta > 0\,, \quad (3)$$

где μ_j, β_j, A_j – центры, параметры полуширин и амплитуды линий спектра. В результате обработки исходных данных требуется оценить значения параметров μ_j, β_j, A_j, в предположении нормального или по Пуассону закона распределения ошибок ε_i:

$$E(\varepsilon_i) = 0\,,\ D(\varepsilon_i) = \sigma^2(\varepsilon_i)\,,\ \sigma(\varepsilon_i) = \sqrt{max(1, y(x_i))}\,. \quad (4)$$

Оценивать параметры резонансов будем по вейвлет-образам спектров.

2. В методе непрерывного вейвлет-преобразования (НВП), при выборе в качестве базисного вейвлета $\psi(x)$, вейвлет-образ сигнала $y(x) = Ag_0(x;\mu,\beta)$, а точнее, коэффициенты его вейвлет-разложения, записываются в виде [1, с. 93]:

$$W_\psi(a,b;y) = a^{-1/2}\int_{-\infty}^{\infty} y(x)\psi\left(\frac{x-b}{a}\right)dx = \int_{-\infty}^{\infty} y(x)\Psi_{ab}(x;\psi)dx, \quad (5)$$

где $\psi(x)$ – базисная вейвлет-функция, а a,b – параметры масштаба и сдвига:

$$\Psi_{ab}(x;\psi) = a^{-1/2}\psi\left(\frac{x-b}{a}\right), \ \left\|\Psi_{ab}(x;\psi)\right\|_{L_2} = \left\|\psi(x)\right\|_{L_2}. \quad (6)$$

Вейвлет-преобразование сводится к вычислению корреляции между функциями $\Psi_{ab}(x;\psi)$ и фрагментами исходного сигнала.

Известно, что в силу коммутирования операции дифференцирования и НВП [2, с. 1155], для вейвлет-преобразований справедливы соотношения:

$$W_\psi\left(a,b;\frac{d^n}{dx^n}y(x)\right) = (-1)^n\int_{-\infty}^{\infty} y(t)\cdot\frac{d^n}{dx^n}\Psi_{ab}(t;\psi)\cdot dt \ , \quad (7)$$

что позволяет перейти от дифференцирования заданного численно исходного спектра $y(x)$ к дифференцированию выписываемого в виде аналитической функции вейвлета $\Psi_{a,b}(t;\psi)$.

3. При преобразовании спектров методом НВП в работе в качестве базисных использованы гауссовы вейвлеты 2-го порядка – $\psi_2(x)$ и $\varphi_2(x)$:

$$\psi_2(x) = (1-x^2)e^{-x^2/2}, \ \varphi_2(x) = 2C_2^{-1}(1-2x^2)e^{-x^2}, \ C_2 = \sqrt{3}\cdot(\pi/2)^{1/4}, \quad (8)$$

а при разметке спектров [3] – базисный гауссов вейвлет 4-го порядка:

$$\varphi_4(x) = 4C_4^{-1}(4x^4 - 12x^2 + 3)e^{-x^2}, \ C_4 = \sqrt{105}\cdot(\pi/2)^{1/4}. \quad (9)$$

Функции $\psi_n(x)$ и $\varphi_n(x)$ вычисляются через производные гауссовых кривых $e^{-x^2/2}$ и e^{-x^2} [1, с. 151]:

$$\psi_n(x)=(-1)^{n+1}\frac{d^n}{dx^n}e^{-x^2/2}\ , \tag{10}$$

$$\varphi_n(x)=\alpha_n C_n^{-1}\frac{d^n}{dx^n}e^{-x^2}\ ,\ C_n=\left\|\varphi_n(x)\right\|_{L_2},\ |\alpha_n|=1,\ n\geq 1. \tag{11}$$

Вейвлеты $\psi_n(x)$ и $\varphi_n(x)$ используются в пакете расширения Wavelet Toolbox системы компьютерной математики Matlab [1, с. 135].

Доказано, что при выборе базисных гауссовых вейвлетов $\psi_n(x)$ 2-го и 4-го порядков [1, с. 151], коэффициенты разложения синглета $y(x)=Ag_0(x;\mu,\beta)$ выписываются в явном виде [3]:

$$W_{\psi_n}(a,b;y)=\frac{A\sqrt{2\pi}\beta}{\sqrt{a}}\left(1+\left(\frac{\beta}{a}\right)^2\right)^{-(2[n/2]+1)/2}\cdot\psi_n\left(\frac{b-\mu}{\sqrt{a^2+\beta^2}}\right),\ n=2,4. \tag{12}$$

Из формулы (12) следует, что рассматриваемые вейвлет-преобразования сохраняют положения одиночных резонансов на оси аргумента.

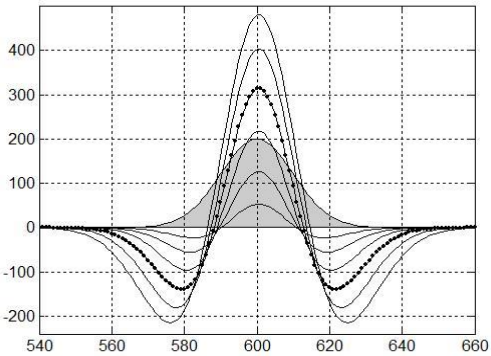


Рисунок 1. Графики синглета $y(x)$ ***и его вейвлет-образов*** $W_{\varphi_2}(a,b;y)$ ***при различных масштабах вейвлетов:*** $a\in\{4,6,8,10,12,14\}$, $\beta=10$

Важно отметить, что метод НВП на основе гауссовых вейвлетов, характеризующихся не менее чем двумя первыми нулевыми моментами [2], позволяет анализировать резонансные пики спектра без учета влияния медленно меняющейся базовой компоненты спектра. Графики используемых в работе базисных вейвлетов напоминают резонансные кривые (рис. 1).

4. Оценим полуширину синглета по двум его вейвлет-разложениям по гауссовым вейвлетам на основе $\psi_2(x)$ при двух различных значениях масштаба. При выборе $\psi_2(x)$ в качестве базисного вейвлета значение коэффициента разложения синглета $y(x) = Ag_0(x;\mu,\beta)$ в точке $b = \mu$, соответствующей центру пика, имеет вид [3]:

$$W_{\psi_2}(a,\mu;y) = A\sqrt{2\pi}\beta a^{5/2} z^{-3},\ z = (a^2+\beta^2)^{1/2}. \qquad (13)$$

Нетрудно видеть, что при использовании различных масштабов a_1, a_2 вейвлета, $0 < a_1 < a_2$, будет справедливо равенство:

$$\frac{W_{\psi_2}(a_1,\mu;y)}{{a_1}^{5/2} {z_1}^{-3}} = \frac{W_{\psi_2}(a_2,\mu;y)}{{a_2}^{5/2} {z_2}^{-3}},$$

где $z_k = ({a_k}^2+\beta^2)^{1/2}$, $k = 1,2$. Для простоты дальнейших выкладок введем обозначения: $w(a_k) = \left|W_{\psi_2}(a_k,\mu;y)\right| > 0$, $k = 1,2$. Тогда получим:

$$\left(\frac{z_1}{z_2}\right)^{3\cdot 2} = \left(\left(\frac{a_1}{a_2}\right)^{5/2} \cdot \frac{w(a_2)}{w(a_1)}\right)^2,\ \frac{{a_1}^2+\beta^2}{{a_2}^2+\beta^2} = \left(\left(\frac{a_1}{a_2}\right)^{5/2} \cdot \frac{w(a_2)}{w(a_1)}\right)^{2/3}$$

Прологарифмируем последнее полученное соотношение:

$$\lambda(a_1,a_2) = ln\left(\frac{{a_1}^2+\beta^2}{{a_2}^2+\beta^2}\right) = \frac{2}{3}\cdot\left(\frac{5}{2}\cdot ln\left(\frac{a_1}{a_2}\right) + ln\left(\frac{w(a_2)}{w(a_1)}\right)\right)\cdot$$

И из равенства $\theta(a_1,a_2)=\frac{a_1^2+\beta^2}{a_2^2+\beta^2}$, где $\theta(a_1,a_2)=e^{\lambda(a_1,a_2)}$, получим искомую оценку значения полуширины синглета:

$$\hat{\beta}=\sqrt{\frac{a_2^2\cdot\theta(a_1,a_2)-a_1^2}{1-\theta(a_1,a_2)}}. \qquad (14)$$

Оценки амплитуды пика $y(x)$ для значений масштабов a_1, a_2 вейвлета в соответствии с формулой (13) будут иметь вид:

$$\hat{A}_k=w(a_k)\cdot\sqrt{a_k}\left(1+(\hat{\beta}/a_k)^2\right)^{3/2}/(\sqrt{2\pi}\hat{\beta}),\ k=1,2. \qquad (15)$$

5. Разберемся с оценкой параметров для случая базисного вейвлета $\varphi_2(x)$. Известно, что с точностью до линейного множителя вейвлеты $\varphi_n(x)$ совпадают с вейвлетами $\psi_n(x\sqrt{2})$ [3], поэтому:

$$W_{\varphi_2}(a,b;y)=2^{1/2}C_2^{-1}\cdot W_{\psi_2}(a,\sqrt{2}b;y_0),$$
$$y_0(x)=y(x/\sqrt{2})=Ag_0(x;\sqrt{2}\mu,\sqrt{2}\beta).$$

Обозначим для простоты изложения через $v(a)$ значение коэффициента $W_{\psi_2}(a,\sqrt{2}\mu;y_0)$ разложения масштабированного синглета $y_0(x)$ в точке его центра [3], $b=\sqrt{2}\mu$: $v(a)=W_{\psi_2}(a,\sqrt{2}\mu;y_0)=2A\sqrt{\pi}\beta a^{5/2}[q(a)]^{-3}$, где $q(a)=(a^2+2\beta^2)^{1/2}$.

Поскольку, как предполагается, заданы разложения синглета для двух значений масштабов a_1, a_2 вейвлета, $0<a_1<a_2$, то справедливы равенства:

$$\frac{W_{\varphi_2}(a_1,\mu;y)}{W_{\varphi_2}(a_2,\mu;y)}=\frac{W_{\psi_2}(a_1,\sqrt{2}\mu;y_0)}{W_{\psi_2}(a_2,\sqrt{2}\mu;y_0)}=\frac{v(a_1)}{v(a_2)}=\frac{a_1^{5/2}q_1^{-3}}{a_2^{5/2}q_2^{-3}},$$

где $q_k=\sqrt{a_k^2+(\sqrt{2}\beta)^2}$, $k=1,2$, и $\left(\frac{q_1}{q_2}\right)^3=\left(\frac{a_1}{a_2}\right)^{5/2}\cdot\frac{v(a_2)}{v(a_1)}$, $k=1,2$.

По аналогии с рассуждениями, проведенными выше (п.4), получим:

$$\left(\frac{q_1}{q_2}\right)^{3\cdot 2}=\left(\left(\frac{a_1}{a_2}\right)^{5/2}\cdot\frac{v(a_2)}{v(a_1)}\right)^2,\ \frac{{a_1}^2+2\beta^2}{{a_2}^2+2\beta^2}=\left(\left(\frac{a_1}{a_2}\right)^{5/2}\cdot\frac{v(a_2)}{v(a_1)}\right)^{2/3}.$$

Прологарифмировав последнее из полученных соотношений:

$$\lambda_0(a_1,a_2)=ln\left(\frac{{a_1}^2+2\beta^2}{{a_2}^2+2\beta^2}\right)=\frac{2}{3}\cdot\left(\frac{5}{2}\cdot ln\left(\frac{a_1}{a_2}\right)+ln\left(\frac{v(a_2)}{v(a_1)}\right)\right),$$

и введя обозначение: $\theta_0(a_1,a_2)=e^{\lambda_0(a_1,a_2)}$, из равенства $\theta_0(a_1,a_2)=\frac{{a_1}^2+2\beta^2}{{a_2}^2+2\beta^2}$ получим оценку значения полуширины синглета:

$$\hat{\beta}=\sqrt{\frac{{a_2}^2\cdot\theta_0(a_1,a_2)-{a_1}^2}{2(1-\theta_0(a_1,a_2))}}\ . \qquad (17)$$

Оценки амплитуды пика $y(x)$ будут иметь вид:

$$\hat{A}_k=\frac{\sqrt{3a_k}(1+(2\hat{\beta}^2/{a_k}^2))^{3/2}\cdot W_{\varphi_2}(a_k,\mu;y)}{4\hat{\beta}\cdot\sqrt[4]{\pi/2}},\ k=1,2. \qquad (18)$$

6. Вследствие численной неустойчивости операции дифференцирования, при обработке зашумленных данных обычно проводят предварительное сглаживание данных, например, гауссовыми фильтрами или сглаживающими полиномиальными фильтрами Савицкого-Голея (SG фильтрами) [4]. Сглаживание спектрометрических данных служит для уменьшения уровня шума в данных и, как следствие, ведет к снижению погрешностей анализа.

Сглаженные SG фильтрами значения спектра вычисляют по значениям локальных аппроксимирующих полиномов, полученных методом наименьших квадратов для точек спектра из соответствующего окна оси аргумента. Коэффициенты сглаживающего SG фильтра определяются только шириной окна сглаживания $(2m+1)$ и выбранным порядком полинома $k<2m+1$. Например, при обработке спектро-

метрических данных обычно достаточно использования сглаживающего кубического SG фильтра $(k=3)$, который в этом случае задается квадратичным полиномом вида [4]:

$$h(s)=\frac{3\{(3m^2+3m-1)-5s^2\}}{(2m+3)(2m+1)(2m-1)},\ s=-m,\dots,m\ . \qquad (19)$$

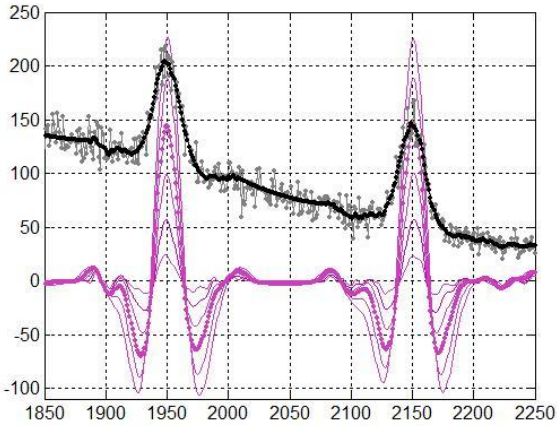


Рисунок 2. Графики зашумленного и сглаженного SG фильтром спектра $y(x)$ ***и вейвлет-образов*** $W_{\varphi_2}(a,b;y)$ ***при различных масштабах вейвлетов:*** $a\in\{4,6,8,10,12,14\}$, $\beta=10$

7. Рассмотрим возможности алгоритма оценивания параметров синглетов на примере. Алгоритм реализован в рамках системы компьютерной математики Matlab.

Модельный спектр, фрагмент графика которого показан на рис.2, задан суперпозицией 4-х гауссовых линий: $Y(x)=\sum_{j=1}^{4}g_j(x)$, – с параметрами $\mu_j=1550+200\cdot(j-1)$, $\beta_j=10$, $A_j=100$, $j=1...4$, базовая кривая $B(x)$ – суммой двух широких гауссианов. Зашумленный квазиреальный спектр смоделирован по закону распределения ошибок по Пуассону. В нижней части рис.2 точками выделен график кривой $W_{\varphi_2}(a,b;y)$, соответствующей масштабу $a=\beta=10$.

При обработке спектра положения центров резонансов μ_j оценивались через абсциссы локальных максимумов кривой $W_{\varphi_4}(a,b;y)$ [3]. Оценки полуширин $\hat{\beta}_{j,med}$ и амплитуд $\hat{A}_{j,med}$ пиков спектра вычислялись через выборочные медианы наборов оценок $\{\hat{\beta}_{js}\}$ и $\{\hat{A}_{js}\}$, полученных для базового гауссова вейвлета $\varphi_2(x)$ при масштабах $0<a_1<a_2$, $a_1, a_2 \in \{6,8,10,12,14\}$. Разброс оценок этих параметров по отдельным резонансам можно проанализировать с помощью значений $\hat{\beta}_{j,min}$, $\hat{\beta}_{j,max}$, $\hat{A}_{j,min}$, $\hat{A}_{j,max}$, приведенных в таблицах 1-3. При обработке данных указанным алгоритмом заметно влияние точности указания центров пиков $\hat{\mu}_j$ на результаты работы алгоритма (см таблицы 2,3).

Таблица 1.

Обработка точных данных, $y_B(x)=Y(x)+B(x)$

j	$\hat{\mu}_j$	$\hat{\beta}_{j,med}$	$\hat{\beta}_{j,min}$	$\hat{\beta}_{j,max}$	$\hat{A}_{j,med}$	$\hat{A}_{j,min}$	$\hat{A}_{j,max}$
1	1551	10.01	9.96	10.09	99.95	99.19	100.61
2	1750	10.02	9.97	10.10	100.26	99.43	100.90
3	1950	10.01	9.95	10.09	99.90	99.18	100.55
4	2151	10.00	9.96	10.07	99.56	98.93	100.22

Таблица 2.

Обработка сглаженных защумленных данных $y(x_i)=y_B(x_i)+\varepsilon_i$

j	$\hat{\mu}_j$	$\hat{\beta}_{j,med}$	$\hat{\beta}_{j,min}$	$\hat{\beta}_{j,max}$	$\hat{A}_{j,med}$	$\hat{A}_{j,min}$	$\hat{A}_{j,max}$
1	1553	8.64	8.26	8.99	89.44	84.67	91.00
2	1751	10.67	10.02	10.98	97.54	89.25	99.69
3	1948	9.94	8.68	10.68	86.67	72.46	90.75
4	2153	9.20	8.60	9.66	92.58	84.88	95.01

Таблица 3.

Обработка сглаженных данных $y(x_i) = y_B(x_i) + \varepsilon_i$ при точно заданных значениях центров пиков

j	$\hat{\mu}_j$	$\hat{\beta}_{j,med}$	$\hat{\beta}_{j,min}$	$\hat{\beta}_{j,max}$	$\hat{A}_{j,med}$	$\hat{A}_{j,min}$	$\hat{A}_{j,max}$
1	1550	9.58	9.49	10.88	95.26	94.54	112.52
2	1750	10.65	9.56	11.07	97.19	83.65	100.01
3	1950	10.89	10.63	11.07	97.13	95.16	99.35
4	2150	10.53	10.19	10.63	102.57	100.06	103.73

Как следует из приведенных численных результатов, предложенный алгоритм оценивания параметров резонансных линий возможно использовать при решении задач обработки спектров излучения.

Список литературы:

1. Дьяконов, В.П. Вейвлеты. От теории к практике. М.: Солон-Р, 2002. – 448 с.
2. Астафьева, Н.М. Вейвлет-анализ: основы теории и примеры применения // УФН. – 1966. – Т. 166. – № 11. – С. 1145-1170.
3. Подосенова, Т.Б. О локализации резонансных линий в задачах обработки спектров [Электронный ресурс] // Электронный научный журнал. – 2019. – № 4 (26). – С. 7-16. URL: http://co2b.ru/uploads/enj.2019.04.pdf
4. Подосенова, Т.Б. О сглаживающих SG фильтрах для задач обработки спектров [Электронный ресурс] // Электронный научный журнал. – 2019. - № 3 (25). – С. 16-24. URL: http://co2b.ru/uploads/enj.2019.03.pdf

ОЦЕНИВАНИЕ ПАРАМЕТРОВ РЕЗОНАНСОВ ПО ВЕЙВЛЕТ-ОБРАЗАМ СПЕКТРОВ ИЗЛУЧЕНИЯ ДЛЯ ГАУССОВЫХ ВЕЙВЛЕТОВ МЛАДШИХ ЧЕТНЫХ ПОРЯДКОВ

Подосенова Татьяна Борисовна
канд. физ.-мат. наук,
старший научный сотрудник,
Московский государственный университет
имени М.В. Ломоносова,
РФ, г. Москва

ESTIMATION OF RESONANCES PARAMETERS ON THE BASE OF THE WAVELET TRANSFORM OF RADIATION SPECTRA FOR GAUSSIAN WAVELETS OF THE SMALLEST EVEN ORDERS

Tatyana Podosenova
Candidate of Science in Physics
and Mathematics, Senior Researcher,
Lomonosov Moscow State University,
Russia, Moscow

Аннотация. В работе предложен способ оценивания значений параметров резонансных линий в спектрах излучения, путем анализа полученных методом непрерывного вейвлет-преобразования вейвлет-образов спектров, с использованием гауссовых вейвлетов в качестве базовых. При получении аналитических оценок параметров использованы вычисленные в точках центров резонансов значения отношений вейвлет-коэффициентов, соответствующие базисным гауссовым вейвлетам двух разных порядков.

Abstract. The paper proposes a method for estimating the values of the parameters of resonance lines in the radiation spectra by analyzing the wavelet images of spectra obtained by the method of continuous wavelet transformation, by using of Gaussian wavelets as the base ones. When obtaining analytical estimates of the parameters, the values of the wavelets coefficients ratios corresponding to the basic Gaussian wavelets of two different orders are calculated at the points of the resonance centers.

Ключевые слова: спектр излучения; резонансная линия; непрерывное вейвлет-преобразование; гауссов вейвлет.

Keywords: radiation spectrum; resonance line; continuous wavelet transform; Gaussian wavelet.

1. Обработка исходных данных – аппаратно регистрируемых спектров излучения $y(x)$ – сводится в итоге к определению параметров суммы $Y(x)$ резонансных унимодальных функций, в предположении нормального или по Пуассону закона распределения ошибок ε_i:

$$y(x)=\{y_i \geq 0,\ y_i = y(x_i) = Y(x_i) + B(x_i) + \varepsilon_i\ , i = 1,...,n\}, \quad (1)$$

$$Y(x) = \sum\nolimits_j A_j g_j(x)\ ,\ g_j(x) = g_0(x;\mu_j,\beta_j)\ , \quad (2)$$

$$g_0(x;\mu,\beta) = e^{-(x-\mu)^2/(2\beta^2)},\ \int_{-\infty}^{\infty} g_0(x;\mu,\beta)dx = \sqrt{2\pi}\beta\ , \quad (3)$$

$$E(\varepsilon_i)=0,\ D(\varepsilon_i)=\sigma^2(\varepsilon_i),\ \sigma(\varepsilon_i)=\sqrt{max(1,y(x_i))}\ , \quad (4)$$

где μ_j, β_j, A_j – центры, параметры полуширин и амплитуды пиков (резонансов), а $B(x_i)$ – гладкая базовая кривая.

2. В методе непрерывного вейвлет-преобразования, при выборе в качестве базисного вейвлета $\psi(x)$, коэффициенты вейвлет-разложения исходного спектра записываются в виде [1, с. 93]:

$$W_\psi(a,b;y) = a^{-1/2}\int_{-\infty}^{\infty} y(t)\psi\left(\frac{t-b}{a}\right)dt\ , \quad (5)$$

где a,b – параметры масштаба и сдвига вейвлета. Для синглета $y(x) = Ag_0(x;\mu,\beta)$ при выборе базисных гауссовых вейвлетов $\psi_n(x)$ 2-го и 4-го порядков [1, с. 151], вейвлет-коэффициенты выписываются в явном виде [2]:

$$W_{\psi_n}(a,b;y) = \frac{A\sqrt{2\pi}\beta}{\sqrt{a}}\left(1+\left(\frac{\beta}{a}\right)^2\right)^{-(2[n/2]+1)/2} \cdot\psi_n\left(\frac{b-\mu}{\sqrt{a^2+\beta^2}}\right),\ n=2,4, \quad (6)$$

$$\psi_2(x) = (1-x^2)e^{-x^2/2}\ ,\ \psi_4(x) = (-x^4+6x^2-3)e^{-x^2/2}. \quad (7)$$

В работе используются также гауссовы вейвлеты $\varphi_n(x)$, $n = 2,4$:

$$\varphi_2(x) = 2C_2^{-1}(1-2x^2)e^{-x^2}\ ,\ C_2 = \sqrt{3}\cdot(\pi/2)^{1/4}, \quad (8)$$

$$\varphi_4(x) = 4C_4^{-1}(4x^4-12x^2+3)e^{-x^2}\ ,\ C_4 = \sqrt{105}\cdot(\pi/2)^{1/4}. \quad (9)$$

Отметим, что гауссовы вейвлеты $\psi_n(x)$ и $\varphi_n(x)$ основаны на вычислении производных гауссовых функций, $e^{-x^2/2}$ и e^{-x^2} соответственно [1, с. 151], и, конечно, различаются масштабами (полуширинами). Гауссовы вейвлеты симметричны относительно своего центра, поэтому локальные максимумы модулей коэффициентов вейвлет-разложения спектров совпадают с положениями одиночных резонансов. Графики функций $\psi_n(x)$ и $\varphi_n(x)$ при четных значениях порядков n похожи формой на резонансные кривые, их аналитические представления можно записать через ортогональные полиномы Эрмита. А поскольку гауссовы вейвлеты имеют не менее двух первых нулевых моментов, они позволяют анализировать резонансные пики спектра без учета влияния достаточно медленной и плавной базовой компоненты спектра.

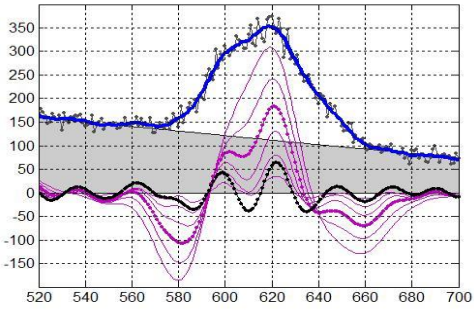


Рисунок 1. Графики кривых $y(x)$, $B(x)$, $\tilde{y}(x)$ ***и вейвлет-образов*** $W_{\varphi_n}(a,b;\tilde{y})$, $n = 2,4$ ***зашумленного спектра*** $\tilde{y}(x)$ ***при различных масштабах вейвлетов:*** $a \in \{4,6,8,10,12,14\}$ ***при*** $n = 2$, $a = 10$ ***при*** $n = 4$, $\beta = 10$

3. Для гауссовых вейвлетов $\psi_n(x)$ при выполнении условия $b-\mu=0$ справедливо: $\psi_2(0)=1,\ \psi_4(0)=-3$. Поэтому для модулей w_2 , w_4 коэффициентов вейвлет-разложения $W_{\psi_n}(a,b;y)$, вычисленных в точке центра синглета $y(x)=Ag_0(x;\mu,\beta)$, справедливы соотношения:

$$w_4 / w_2 = 3a^2 / (a^2+\beta^2), \tag{10}$$

$$w_2 = W_{\psi_2}(a,\mu;y) = A\sqrt{2\pi}\beta a^{5/2} z^{-3},$$
$$w_4 = -W_{\psi_4}(a,\mu;y) = 3A\sqrt{2\pi}\beta a^{9/2} z^{-5},$$

где $z=(a^2+\beta^2)^{1/2}$. Оценки параметров синглета окончательно имеют вид:

$$\hat{\beta} = a\left(\frac{3w_2}{w_4}-1\right)^{1/2},\ \hat{A} = w_2 a^{1/2}\left(1+(\hat{\beta}/a)^2\right)^{3/2} / (\sqrt{2\pi}\hat{\beta})\ . \tag{11}$$

4. Для гауссовых вейвлетов $\varphi_n(x)$ при значениях $b=\mu$ выполняется: $\varphi_2(0)=(2/C_2)>0$, $\varphi_4(0)=(12/C_4)>0$ [2]. И поскольку с точностью до линейного множителя базисные вейвлеты $\varphi_n(x)$ совпадают с вейвлетами $\psi_n(x\sqrt{2})$, то получим:

$$W_{\varphi_2}(a,b;y) = 2^{1/2} C_2^{-1} \cdot W_{\psi_2}(a,\sqrt{2}\,b;y_0)\ ,$$

$$W_{\varphi_4}(a,b;y) = -2^{3/2} C_4^{-1} \cdot W_{\psi_4}(a,\sqrt{2}\,b;y_0)\ ,$$

где $y_0(x)=y(x/\sqrt{2})=Ag_0(x;\sqrt{2}\mu,\sqrt{2}\beta)$.

Окончательно формулы для оценивания параметров пика с использованием базовых гауссовых вейвлетов $\varphi_n(x)$ имеют вид [2]:

$$\hat{\beta} = \frac{a}{\sqrt{2}}\left(\frac{6}{\sqrt{35}}\cdot\frac{q_2}{q_4}-1\right)^{1/2},\ \hat{A} = \frac{q_2\sqrt{3a}(1+(2\hat{\beta}^2/a^2))^{3/2}}{4\hat{\beta}\cdot\sqrt[4]{\pi/2}}\ , \tag{12}$$

$$q_2 = \sqrt{2}C_2^{-1}\tilde{w}_2 > 0\ ,\ \tilde{w}_2 = W_{\psi_2}(a,\sqrt{2}\mu; y_0) = 2A\sqrt{\pi}\beta a^{5/2} z_0^{-3}\ ,$$

$$q_4 = 2\sqrt{2}C_4^{-1}\tilde{w}_4 > 0\ ,\ \tilde{w}_4 = -W_{\psi_4}(a,\sqrt{2}\mu; y_0) = 6A\sqrt{\pi}\beta a^{9/2} z_0^{-5}\ ,$$

где $z_0 = (a^2 + 2\beta^2)^{1/2}$.

5. На модельных примерах протестируем качество предложенного алгоритма оценивания параметров синглетов. Алгоритм реализован в рамках системы компьютерной математики Matlab, на базе вейвлетов $\varphi_n(x)$, включенных в пакет расширения Wavelet Toolbox [1, с. 135]. Рассмотрим синглет $y(x)$ с параметрами $\mu = 550$, $\beta = 16$, $A = 200$. Квазиреальные зашумленные спектры $\tilde{y}(x)$ будем формировать с учетом нормального (либо по Пуассону) закона распределения ошибок ε_i (4):

$$\tilde{y}(x) = \{\tilde{y}_i = y_i + \varepsilon_i\ , i = 1,...,n\}\ . \qquad (13)$$

Затем квазиреальные спектры сгладим гауссовыми фильтрами, а полученные их вейвлет-разложения обработаем по алгоритму (п.4), на основе базисных вейвлетов $\varphi_2(x), \varphi_4(x)$. При фиксированном значении масштаба вейвлета за оценки положений центров резонансов возьмем аргументы точек локальных максимумов вейвлет-образов спектров.

В результате при значении масштаба вейвлетов $a = 16$, например, для невозмущенного модельного синглета были получены оценки параметров: $\hat{\beta} = 16.02$, $\hat{A} = 200.02$, а для двух зашумленных спектров $\tilde{y}(x)$ – оценки $\hat{\beta} = 15.29$, $\hat{A} = 198.47$ и $\hat{\beta} = 15.62$, $\hat{A} = 195.86$.

Рассмотрим также случай, когда модельный спектр есть сумма базовой и резонансных компонент: $y(x) = Ag_0(x;\mu,\beta) + B(x)$, а базовая компонента спектра $B(x)$ задана в виде широкой гауссовой кривой с параметрами $\mu_B = 350$, $\beta_B = 150$, $A_B = 100$.

По описанному выше алгоритму при значении $a = 16$ для невозмущенного модельного спектра получены оценки $\hat{\beta} = 15.98$, $\hat{A} = 198.89$, а для двух зашумленных спектров – $\hat{\beta} = 15.80$, $\hat{A} = 194.84$ и $\hat{\beta} = 16.46$, $\hat{A} = 195.49$.

Как следует из приведенных численных результатов, предложенный алгоритм оценивания параметров резонансных линий возможно использовать при решении задач обработки спектров излучения.

Список литературы:

1. Дьяконов, В.П. Вейвлеты. От теории к практике. М.: Солон-Р, 2002. – 448 с.
2. Подосенова, Т.Б. Оценивание параметров резонансов с помощью CWT преобразований // Развитие науки и образования в современном мире: сб. тр. науч.-практич. конф. – АР-Консалт Москва, 2018. – С. 17 – 23.

РАЗДЕЛ 3.

МЕХАНИКА

3.1. МЕХАНИКА ЖИДКОСТИ, ГАЗА И ПЛАЗМЫ

АНАЛИЗ ОТЕЧЕСТВЕННОГО И ЗАРУБЕЖНОГО ОПЫТА ПРИМЕНЕНИЯ ТЕПЛОВЫХ МЕТОДОВ ВОЗДЕЙСТВИЯ

Борто Василий Иосифович
заместитель начальника
нефтепромысла по производству,
ООО «Няганьнефть»,
Тюменский индустриальный университет,
РФ, г. Тюмень

Аннотация. Проблема разработки месторождений тяжелой нефти заключается в неблагоприятном соотношении подвижностей нефти и вытесняющего агента. Тепловое воздействие относится к методам первой группы воздействия. Проведение анализа отечественного и зарубежного опыта применения тепловых методов воздействия актуально для условий высоковязких нефтей Русского месторождения. В результате анализа мировой практики применения тепловых методов воздействия на вязкие нефти, предложена схема, характеризующая эффективность тепловых методов, ранжированных в зависимости от рисков, связанных с их реализацией.

Abstract. The problem of developing heavy oil deposits lies in the unfavorable ratio of the mobility of oil and the displacing agent. Thermal exposure refers to the methods of the first group of exposure. The analysis of domestic and foreign experience in the application of thermal methods of exposure is relevant for the conditions of high-viscosity oils of the Russian field. As a result of the analysis of the world practice of applying thermal methods of influence on viscous oils, a scheme is proposed that characterizes the effectiveness of thermal methods ranked depending on the risks associated with their implementation.

Ключевые слова: месторождение; пласт; тепловой метод; методы воздействия; Русское месторождение; нефтеотдача.

Keywords: deposit; formation; body method; impact methods; russian deposit; oil recovery.

Проблема разработки месторождений тяжелой нефти заключается в неблагоприятном соотношении подвижностей вытесняемого (нефти) и вытесняющего агентов (например, вода). Разница в десятки и сотни раз значений вязкости способна существенно снизить эффективность вытеснения более вязкой фазы. Изменить данную диспропорцию можно путем уменьшения вязкости самой нефти, либо путем увеличения вязкости вытесняющего агента, либо изменяя эти величины одновременно. К методам первой группы относится тепловое воздействие, реализация смешивающегося и частично смешивающегося вытеснения.

Наибольшее распространение тепловые методы получили в Канаде, США (Калифорния), Венесуэле и Индонезии (Balol field, Coalinga, Lost Hills, Christina Lake, San Ardo, Bellevue). Все применяемые тепловые методы можно разделить на две большие группы, отличающиеся между собой способом передачи тепловой энергии в пласт: в одной из них теплоноситель готовится на поверхности и подается в скважину через устьевое оборудование, в другой тепло создается непосредственно в скважине или в пласте.

В качестве теплоносителей для нагнетания в пласт применяются вода и насыщенный водяной пар. Именно эти теплоносители характеризуются наибольшей среди известных рабочих агентов теплоёмкостью и, следовательно, дают возможность обеспечить лучшую эффективность теплового воздействия на пласт. С точки зрения эффективности снижения вязкости нефти, предпочтительным является водяной пар.

Процесс SAGD, разработанный в 1977-78 гг. Роджером Батлером, предполагает бурение пары горизонтальных скважин на расстоянии 4-6 метров одна над другой. Пар нагнетается через верхнюю скважину, отдавая тепловую энергию пластовой системе, понижает вязкость нефти. Добыча при этом осуществляется через нижнюю скважину.

В ходе закачки пара формируется паровая камера, по стенкам которой к добывающей скважине стекает нагретая нефть вместе с водяным конденсатом (Рисунок 1).

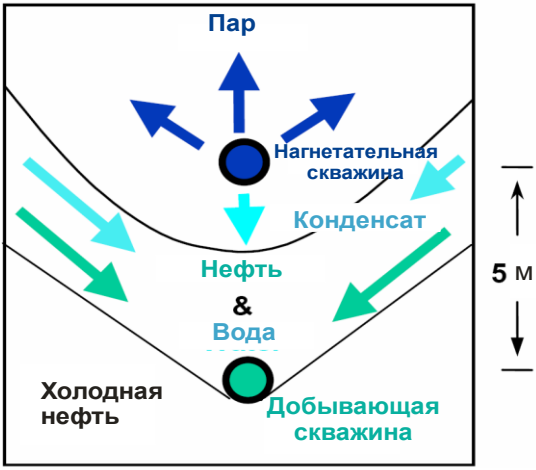


Рисунок 1. Схема процесса SAGD

Одной из разновидностей SAGD является реализация данного метода с использованием одной горизонтальной скважины SW-SAGD (Single Well SAGD). В этом методе пар и нефть закачивается и добывается в одно и то же время через одну и ту же одиночную горизонтальную скважину. Это стало возможным за счет технологии Insulated Concentric Coiled Tubing, разработанной NOWSCO Well Service Ltd. Пар доставляется в самый конец горизонтальной скважины (называемый «toe», «носок») через теплоизолированную трубу без участия НКТ.

Для повышения эффективности SAGD в закачиваемый пар добавляют углеводородные компоненты (C1-C5), данная технология называется ES-SAGD. В результате удачным образом сочетаются преимущества тепловых методов и применения растворителей (Рисунок 2).

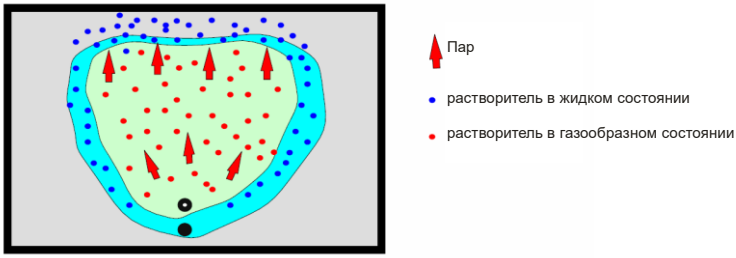


Рисунок 2. Схема процесса ES-SAGD

В технологии SAS (Solvent Alternating with Steam) также используется пар и углеводородные растворители, но его отличие от ES-SAGD заключается в режиме нагнетания агентов.

Метод VAPEX заключается в закачке в качестве вытесняющего агента парообразного растворителя (Рисунок 3). Идея процесса заключается в том, что парообразный растворитель закачивается в пласт и растворяется в нефти, уменьшая ее вязкость. Технология VAPEX, также как и SAGD, чувствительна к вертикальной сообщаемости объекта воздействия. Метод имеет существенные недостатки. Прежде всего, это крайне медленный процесс, поскольку основной механизм нефтеотдачи связан с «разжижением нефти» за счет молекулярной диффузии растворителя в высоковязкую нефть. Во-вторых, он является высокозатратным из-за необходимости использования растворителей. Эти два фактора, по всей видимости, и препятствуют не только промышленному, но и пилотному применению VAPEX на месторождениях высоковязкой нефти.

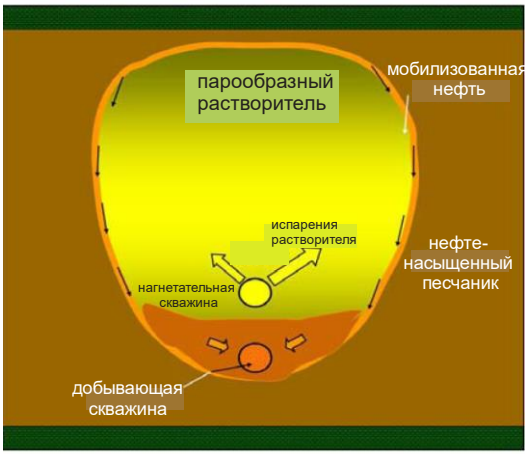


Рисунок 3. Схема процесса VAPEX

Среди термических методов, в которых тепловая энергия воспроизводится непосредственно в пласте, можно выделить сухое, влажное и сверхвлажное внутрипластовое горение (ВПГ), основанное на инициализации в пласте очага экзотермической окислительно-восстановительной реакции и продвижении его по пласту. Несомненным преимуществом данного метода является возможность использования его в широком диапазоне глубин залегания продуктивных пластов. При этом методу

характерны и существенные недостатки, среди которых можно выделить сложность контроля процесса горения и, как следствие, низкий охват пласта воздействием, технологические проблемы, связанные с повышенными температурами и опасностью образования взрывоопасной смеси в добывающих скважинах и т.д.

Внутрипластовое горение используется при таких же системах разработки, как и традиционное заводнение, однако в последнее время разработаны модификации данного метода, сочетающие использование горизонтальных и вертикальных скважин и позволяющие устранить ряд присущих этому процессу недостатков. Основными изменениями технологии внутрипластового горения можно назвать попытки усиления вертикальной составляющей при продвижении очага горения и, как следствие, увеличение охвата пласта воздействием. В технологии TDC (Top-Down Combustion) закачка воздуха осуществляется через вертикальные скважины, перфорируемые у самой кровли продуктивного интервала, добывающие горизонтальные, наоборот, располагаются у подошвы продуктивного пласта (Bellevue, Каражанбас, Balol) (Рисунок 4), в результате очаг горения движется от кровли к подошве залежи. Применение метода TDC и THAI возможно лишь в условиях достаточно монолитного разреза.

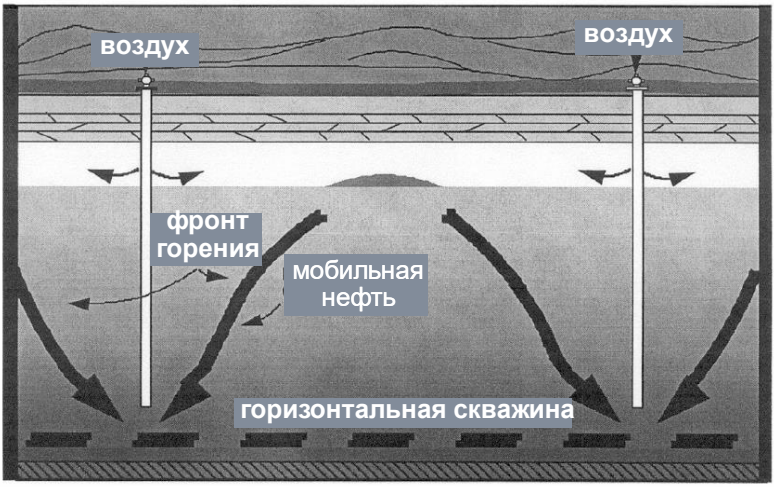


Рисунок 4. Схема осуществления внутрипластового горения по технологии TDC

В результате анализа мировой практики применения тепловых методов воздействия на вязкие нефти, предложена схема, характеризующая эффективность тепловых методов, ранжированных в зависимости от рисков, связанных с их реализацией (Рисунок 5).

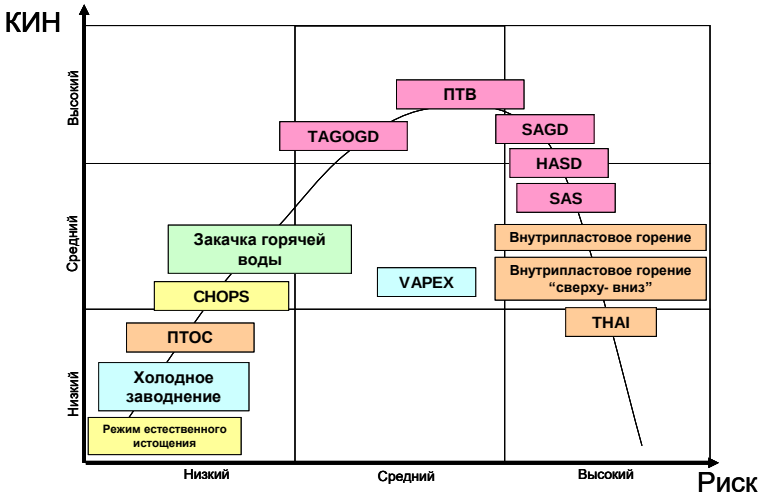


Рисунок 5. Эффективность тепловых методов воздействия на пласт в зависимости от риска и достигаемого КИН

Список литературы:

1. Закиров С.Н., Индрупский И.М. Новые принципы и технологии разработки месторождений нефти и газа. Часть 2; – , 2009. – 488 с.
2. Дополнения к технологической схеме разработки Русского месторождения, 2021.
3. Булатов А.И. Заканчивание нефтяных и газовых скважин: теория и практика / А.И. Булатов, О.В. Савенок. – Краснодар: Просвещение-Юг, 2010. – 539 с.

ИССЛЕДОВАНИЯ НА ОПРЕДЕЛЕНИЕ ПРОФИЛЯ ПРИТОКА С ИСПОЛЬЗОВАНИЕМ ИНДИКАТОРОВ ПРИТОКА

Юдин Дмитрий Викторович
ведущий инженер ЦДНГ,
Тюменский индустриальный университет,
РФ, г. Тюмень

Аннотация. В статье проведен анализ исследований горизонтальных скважин на Русском месторождении с помощью устройства поинтервального мониторинга притока, которое применяется в нефтяных, газовых и водозаборных скважинах и работает в среде минерализованной пластовой воды, нефти, природного газа, конденсата и других скважинных флюидах. В результате установлено, что проведение определения профиля притока при помощи УПМП показывает достоверные результаты, подтверждается работа дополнительных стволов многозабойных скважин.

Abstract. The article analyzes the studies of horizontal wells at the Russian field using a device for interval monitoring of inflow, which is used in oil, gas and water intake wells and works in the environment of mineralized reservoir water, oil, natural gas, condensate and other borehole fluids. As a result, it was found that the determination of the inflow profile with the help of UPMP shows reliable results, the work of additional trunks of multihole wells is confirmed.

Ключевые слова: горизонтальная скважина; ГС; Русское месторождение; УПМП; залежь; дебит; трассеры; устройство поинтервального мониторинга притока.

Keywords: horizontal well; GS; Russian deposit; UPMP; deposit; flow rate; tracers; device for interval monitoring of inflow.

Одним из перспективных методов интенсификации добычи нефти и увеличения полноты её извлечения из недр является разработка месторождений с использованием горизонтальных скважин (ГС).

На Русском месторождении в добыче перебывало 230 горизонтальных скважин. Основная часть эксплуатационного фонда скважин месторождения пробурена в 2016-2020 гг. Максимальный дебит нефти (234,5 т/сут) был зафиксирован у скважины № 2Г в январе 2009 года. Опыт эксплуатации залежи горизонтальными скважинами доказал

свою жизнеспособность, их дебиты оказались на порядок выше дебитов наклонно-направленных скважин.

На скважинах Русского месторождения проводились исследования по определению профиля притока, интервалов работы фильтра и технического состояния скважины. Данные получены с комплекса PLT+ включающего датчики термометрии, манометрии, СТИ, ГК, ЛМ, резистивиметр и объемный влагомер. Замеры выполнены на спуске, подъеме в режиме компрессирования и в остановленной скважине.

Профиль притока распределен равномерно по всему горизонтальному участку, состав флюида – нефть. В местах разделения пластов глинами отмечается более интенсивное поступление флюида. Данный факт может быть связан с особенностями осадконакопления, либо с течением флюида по заколонному пространству фильтра и выходом в интервалах перекрытия пакером.

В целях проведения исследований на определение профиля притока на горизонтальных скважинах Русского месторождения использовалось устройство поинтервального мониторинга притока (далее – устройство, УПМП). Внешний вид устройства приведен на рисунке 1.

Рисунок 1. Внешний вид устройства

Устройство поинтервального мониторинга притока применяется в нефтяных, газовых и водозаборных скважинах и работает в среде минерализованной пластовой воды, нефти, природного газа, конденсата и других скважинных флюидах. УПМП содержит камеру для установки в нее индикаторных пластин с трассерами-метками для определения дебита нефти из различных интервалов, а также определения мест прорыва воды для последующей возможной изоляции соответствующих интервалов. Различные участки скважины оборудованы

различными трассерами, отличающимися друг от друга физическими характеристиками.

Трассеры могут высвобождаться либо только в пластовой воде, либо только в пластовой нефти. Во время освоения скважины нефтерастворимые матрицы растворяются и выделяют трассера-метки. При прорыве воды по какому-либо интервалу скважины растворяются водорастворимые матрицы с выделением соответствующих трассеров-меток. Схема установки УПМП приведена на рисунке 2.

Рисунок 2. Схема установки УПМП

Систематический отбор поверхностных проб во время работы скважины и их анализ на наличие трассеров в пластовом флюиде дает возможность не только определить работающие интервалы во время освоения, но и время и место прорыва воды. Стоит отметить, что профилирование притока проводится на рабочем режиме скважины без искажения картины профиля притока и не требует остановок для взятия проб.

Лабораторные исследования проб на обнаружение трассеров проводиться двумя дублирующими методами.

Первый метод основан на получении оптико-микроскопических изображений трассеров в режиме флуоресценции на четырех длинах волн (405, 488, 561 и 640 нм). Применяемое оборудование для проведения исследования – Конфокальный флуоресцентный микроскоп FEI CorrSight. Определение геометрических характеристик обнаруженных объектов проводится с помощью ПО ImageJ (Рисунок 3).

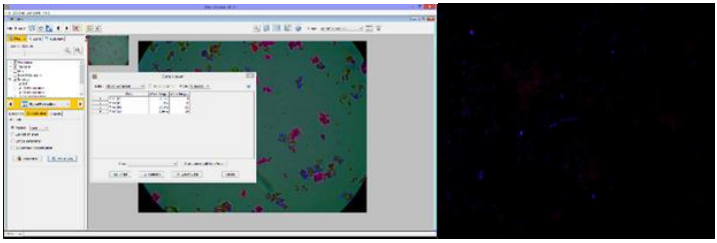


Рисунок 3. Обработка образцов изображений трассеров с помощью ПО

Второй дублирующий анализ проводится методом растровой электронной микроскопии (РЭМ) в режиме высокого вакуума с электронно-зондовым микрорентгеноспектральным анализом элементного состава трассеров. Применяемое оборудования для проведения исследования – Однолучевой сканирующий электронный микроскоп с приставкой-микротомом FEI Teneo (Рисунок 4).

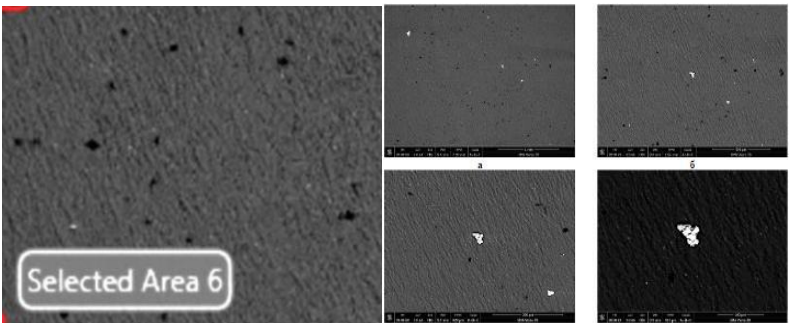


Рисунок 4. Электронно-микроскопические изображения трассеров

Далее на основе полученных результатов по концентрации трассеров определяется поинтервальный профиль притока по нефти и воде.

На Русском месторождении были выполнены пять исследований при освоении пяти скважин. Полученные данные были сопоставлены с аналитическим расчетом продуктивности по данным ГИС выполненных во время бурения. В целом отмечается хорошая сходимость данных ГИС и ИП по распределению продуктивности в горизонтальных скважинах.

В середине 2018 г. в одной из исследуемых горизонтальных скважин был зафиксирован рост обводненности до 30 %, при стартовой величине 5.5 %. Учитывая тот факт, что горизонтальный участок ствола скважины отделен от ВНК выдержанной глинистой перемычкой, было принято решение начать закачку трассера в скважину – единственная нагнетательная скважина, работающая в непосредственной близости (рисунок 5).

Концентрация закачиваемого трассера на нагнетательной скважине составляла 4.8 г/л. По результатам отбора проб выявлен быстрый приход трассера незначительной концентрации в два этапа (рисунок 5). Установлено, что незначительный объем воды движется по каналам высокой проводимости (более 5 Дарси).

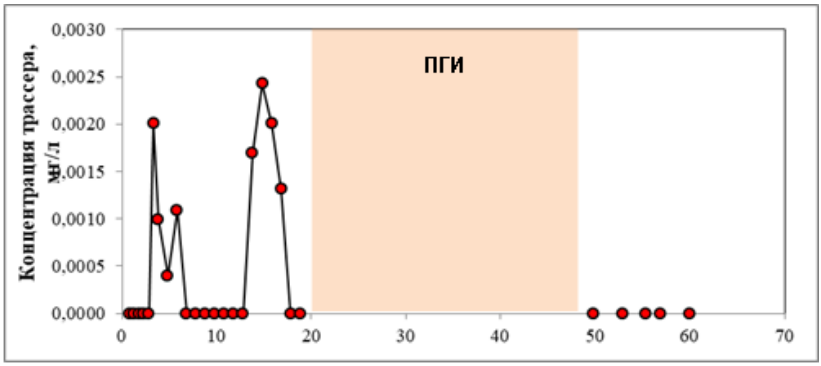
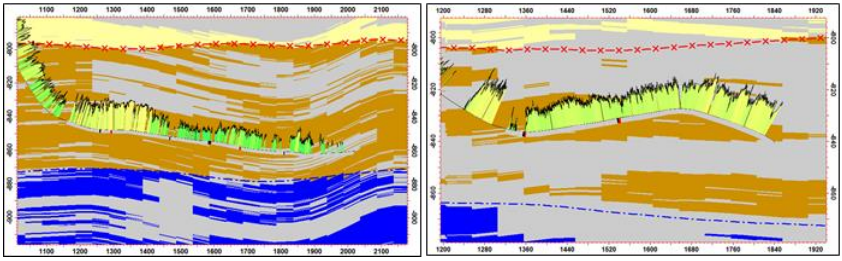


Рисунок 5. Результаты отбора проб в исследуемой скважине

В процессе отбора проб было выполнено ПГИ на исследуемой скважине. Согласно полученному профилю притока, обводнение продукции происходит по пласту ПК2, в который проведена нагнетательная скважина. Таким образом, результаты проведенных исследований позволили однозначно определить источник обводнения скважины – закачиваемая вода в скважину.

Результаты ОПП при помощи индикаторов в исследуемой скважине противоположны данным ГИС. Первый интервал (ближе к «пятке») скважины значительно эффективнее второго. Вероятной причиной может быть характерная траектория горизонтального окончания скважины. Как видно на рисунке 6, вторая половина ГС пробурена с загибом вниз и, несмотря на более лучшие ФЕС, из этого интервала получен меньший приток.



а) б)

Рисунок 6. Результаты ОПП при помощи индикаторов

Вторая скважина с большими отклонениями распределения притока по ГИС и ОПП имеет ровную траекторию, однако, с существенными изменениями ФЕС по стволу (рисунок 6). В целом существенное преимущество первых интервалов фильтра, в добычных показателях, отражается и в результатах ГИС и в результатах ОПП. Стоит так же отметить, что по конструкции скважина имеет 5, изолированных друг от друга пакерами, интервалов, однако, только в двух из них установлены ИП, что могло повлиять на качество результатов в количественном понимании характера притока.

Стоит так же отметить, что по результатам проведенных исследований ОПП в двуствольной скважине подтверждается работа боковой скважины, ее вклад в общий дебит скважины составляет порядка 41 % (по ГИС 25.7%). Различия в распределении притока по ГИС и ОПП, вероятно, связано с особенностью геометрии основного (с перегибом) и бокового (ровный, плавно нисходящий) стволов. Сопоставление и результаты распределения притока по ГИС и ОПП представлены на рисунке 7.

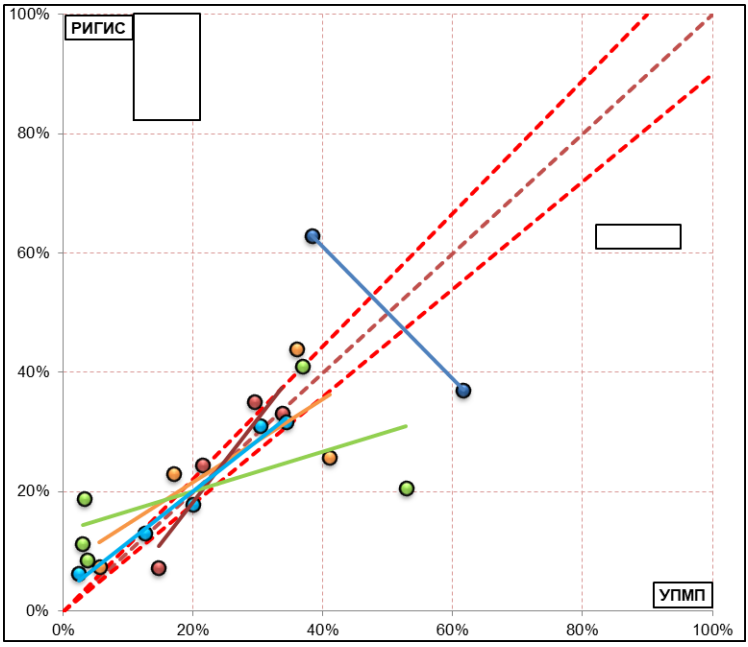


Рисунок 7. Кросс-плот сопоставления распределения продуктивности по ГИС и ОПП

На основании вышеизложенного можно сделать следующие выводы:

- проведение определения профиля притока при помощи УПМП показывает достоверные результаты;
- при помощи УПМП подтверждается работа дополнительных стволов многозабойных скважин, что доказывает эффективность бурения МЗС.

Список литературы:

1. Ситников А.Н., Пустовских А.А., Асмандияров Р.Н., Гильманов Р.Р., Шеремеев А.Ю., Зулькарниев Р.З., 2015. Создание цифровых информационных систем для оптимизации процесса формирования комплексных программ ГТМ. Статья SPE 176561 на Российской нефтегазовой технической конференции SPE, 26 – 28 октября, Москва, Россия.
2. Мищенко, И.Т. Сборник задач по технике нефтедобычи / И.Т. Мищенко, В.А. Сахаров, В.Б. Грон, Г.И. Богомольный. – М.: – 2-е изд., доп. «Недра», 1984. – 272 с.
3. Дополнения к технологической схеме разработки Русского месторождения, 2021.

НАУЧНЫЙ ФОРУМ:
ТЕХНИЧЕСКИЕ И ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ

Сборник статей по материалам LVII международной научно-практической конференции

№ 7 (57)
Октябрь 2022 г.

В авторской редакции

Подписано в печать 06.10.22. Формат бумаги 60x84/16.
Бумага офсет №1. Гарнитура Times. Печать цифровая.
Усл. печ. л. 3,875. Тираж 550 экз.

Издательство «МЦНО»
123098, г. Москва, ул. Маршала Василевского, дом 5, корпус 1, к. 74
E-mail: tech@nauchforum.ru

Отпечатано в полном соответствии с качеством предоставленного оригинал-макета в типографии «Allprint»
630004, г. Новосибирск, Вокзальная магистраль, 3

16+

НАУЧНЫЙ
ФОРУМ
nauchforum.ru