ISSN 2225-5435

Вестник УрФО.

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 1(55) / 2025

УЧРЕДИТЕЛИ
ФГАОУ ВО «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИУ)»

ПРЕДСЕДАТЕЛЬ РЕДАКЦИОННОГО СОВЕТА
ЧУВАРДИН О. П.,
руководитель Управления Федеральной службы по техническому и экспортному контролю России по Уральскому федеральному округу

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

ВЫПУСКАЮЩИЙ РЕДАКТОР
СОГРИН Е. К.

ОТВЕТСТВЕННЫЙ СЕКРЕТАРЬ
АНДРИАДИС Е. Ю.

ВЁРСТКА
ПЕЧЕНКИН В. А.

КОРРЕКТОР
ФЁДОРОВ В. С.

Подписной индекс 73852 в каталоге «Почта России»

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

Свидетельство ПИ № ФС77-65765 от 20.05.2016

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

16+

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

РЕДАКЦИОННЫЙ СОВЕТ:

БАРАНКОВА И. И.,
д. т. н., профессор, зав. кафедрой «Информатика и информационная безопасность», Магнитогорский государственный технический университет им. Г. И. Носова (г. Магнитогорск);

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

ВОЙТОВИЧ Н. И.,
д. т. н., профессор, профессор кафедры «Радиоэлектроника и системы связи», Южно-Уральский государственный университет (национальный исследовательский университет) (г. Челябинск);

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

ДИК Д. И.,
к. т. н., доцент, зав. кафедрой «Безопасность информационных и автоматизированных систем», Курганский государственный университет (г. Курган);

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

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

МЕЛЬНИКОВ А. В.,
д. т. н., профессор, директор Югорского научно-исследовательского института информационных технологий (г. Ханты-Мансийск);

МИНБАЛЕЕВ А. В.,
д. ю. н., доцент, зав. кафедрой «Информационное право и цифровые технологии», Московский государственный юридический университет им. О. Е. Кутафина (МГЮА, г. Москва);

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

РУЧАЙ А.Н.,
д.т.н., доцент, зав. кафедрой «Компьютерная безопасность и прикладная алгебра», Челябинский государственный университет (г. Челябинск);

ХОРЕВ А. А.,
д. т. н., профессор, зав. кафедрой «Информационная безопасность», Национальный исследовательский университет «Московский институт электронной техники» (г. Москва, г. Зеленоград);

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

Journal of the Ural Federal District.

ISSN 2225-5435

INFORMATION SECURITY

№ 1(55) / 2025

FOUNDER
SOUTH URAL STATE UNIVERSITY (NIU)

CHAIRMAN OF THE EDITORIAL BOARD
CHUVARDIN O. P.,
Head of Department Federal Service for Technical and Export Control of Russia for the Urals Federal District

CHIEF EDITOR
SOKOLOV A.N.,
Ph.D., Associate Professor, Head of Department «Information Protection», South Ural State University (National Research University) (Chelyabinsk city)

PRODUCING EDITOR
SOGRIN E. K.

LAYOUT
PECHENKIN V. A.

PROOFREADING
FEDOROV V. S.

Subscription index 73852 in the «Russian Post» catalog

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

Certificate
PI No. ФС77-65765 dd. 05/20/2016

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

16+

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

EDITORIAL COUNCIL:

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

VASILYEV V. I.,
Doctor of Technical Sciences, Professor, Professor of the Department «Computer Science and Information Protection», Ufa State Aviation Technical University (Ufa city);

VOITOVICH N. I.,
Doctor of Technical Sciences, Professor, Professor of the Department «Radioelectronics and Communication Systems», South Ural State University (National Research University) (Chelyabinsk city);

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

DIK D. I.,
Ph.D., Associate Professor, Head of Department «Security of information and automated systems», Kurgan State University (Kurgan city);

ZAHAROV A. A.,
Doctor of Technical Sciences, Professor, Head Basic Department of «Security information technologies smart city», Tyumen State University (Tyumen city);

ZYRYANOVA T. Y.,
Ph.D., Associate Professor, Head of Department «Information Technologies and Information Protection», Ural State University ways of communication (Ekaterinburg city);

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

MINBALEEV A.V.,
Doctor of Law, Associate Professor, Head of Department of «Information Law and Digital Technologies», Moscow State Law University. O. E.Kutafina (Moscow city);

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

RUCHAY A.N.,
Doctor of Technical Sciences, Associate Professor, Head of the Department "Computer Security and Applied Algebra", Chelyabinsk State University (Chelyabinsk city);

HOREV A. A.,
Doctor of Technical Sciences, Professor, Head of Department of «Information Security», National Research University «Moscow Institute of Electronic Technology» (Moscow, the city of Zelenograd);

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

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ОБРАБОТКА ИНФОРМАЦИИ

АНДРЕЕВ А. М., ПОРШНЕВ С. В.
Информационная модель процесса анализа арбитражных судебных решений, проводимого с целью решения задач финансового мониторинга 5

ФАТИН А. Д.
Построение модели адаптивности киберфизических систем: кластеризация, изоляция и реконфигурация 21

ЯПАРОВ Д. Д., КАРМАНОВ Д. Е., ЯПАРОВА Н. М.
Метод обработки информации для прогнозирования степени восстановления металлов на основе нейросетевых технологий 29

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

СЕНЦОВА А. Ю., АРСЛАНОВА Г. И., РУСИНОВА Д. С.
Метод многокритериального выбора средств защиты информации 37

КОСТЮЧЕНКО К. Л., ВАНДЫШЕВ И. С.
Появление новых угроз безопасности информации при применении дронов 45

ЦУКАНОВ А. С., СОКОЛОВ А. Н.
Оценка полноты применяемых методов при внешнем тестировании на проникновение с учетом возможностей нарушителя 55

КУШНИР Н. В., ЯЦКЕВИЧ Е. С., ВЛАСЕНКО А. В., КОПЦОВ С. В.
Передовые подходы к оценке защищенности объектов критической информационной инфраструктуры 62

IN THIS ISSUE

SYSTEM ANALYSIS, MANAGEMENT AND INFORMATION PROCESSING

ANDREEV A. M., PORSHNEV S. V.
Information model of the process of analysis of arbitration court decisions, carried out for the purpose of solving financial monitoring problems 5

FATIN A. D.
Building a model of adaptability of cyberphysical systems: clusterization, isolation and reconfiguration 21

YAPAROV D. D., KARMANOV D. E., YAPAROVA N. M.
Information processing method for forecasting the degree of metal recovery based on neural network technologies 29

METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

SENTSOVA A. U., ARSLANOVA G. I., RUSINOVA D. S.
The method of multi-criteria selection of information security tools. 37

KOSTYUCHENKO K. L., VANDYSHEV I. S.
The emergence of new threats to information security when using drones 45

TSUKANOV A. S., SOKOLOV A. N.
Assessment of the completeness of the methods used in external penetration testing 55

KUSHNIR N. V., YATSKEVICH E. S., VLASENKO A. V., KOPTSOV S. V.
Advanced approaches to assessing the security of critical information infrastructure facilities 62

УДК 004.021 Вестник УрФО № 1(55) / 2025, с. 5–20

Андреев А. М., Поршнев С. В.

10.14529/secur250101

ИНФОРМАЦИОННАЯ МОДЕЛЬ ПРОЦЕССА АНАЛИЗА АРБИТРАЖНЫХ СУДЕБНЫХ РЕШЕНИЙ, ПРОВОДИМОГО С ЦЕЛЬЮ РЕШЕНИЯ ЗАДАЧ ФИНАНСОВОГО МОНИТОРИНГА

В статье проведен анализ нормативно-правовых актов, регламентирующих деятельность Федеральной службы по финансовому мониторингу по противодействию незаконным финансовым операциям и ее взаимодействие с иными государственными органами Российской Федерации, одним из видов которых являются мнимые сделки, легализуемые через решения арбитражных судов. Изучен опыт аналитической деятельности, осуществляемой специалистами в области финансового мониторинга по исследованию данных, содержащихся в указанных источниках информации и построена информационная модель процесса изучения решений арбитражных судов. На основе анализа данной модели сформирован перечень функций, которые должны иметь соответствующие информационные ресурсы, предназначенные для автоматизированного анализа арбитражных судебных решений. Проведен анализ имеющегося функционала, предоставляемого аналитикам известными Интернет-ресурсами, предназначенными для автоматизации деятельности по финансовому мониторингу, и обнаружено, что в составе данных Интернет-ресурсов отсутствуют инструменты для автоматического анализа текстов арбитражных дел. В этой связи сделан вывод об актуальности задачи разработки подобного инструмента на основе использования методов машинного обучения, активно применяемого сегодня в задаче анализа текстовой информации.

Ключевые слова: *Росфинмониторинг, 115-ФЗ, ПОД/ФТ, анализ арбитражных судебных дел, машинное обучение.*

INFORMATION MODEL OF THE PROCESS OF ANALYSIS OF ARBITRATION COURT DECISIONS, CARRIED OUT FOR THE PURPOSE OF SOLVING FINANCIAL MONITORING PROBLEMS

The article analyzes the legal acts governing the activities of the Federal Financial Monitoring Service to combat illegal financial transactions and its interaction with other government agencies of the Russian Federation, one of the types of which are fictitious transactions legalized through decisions of arbitration courts. The experience of analytical activities carried out by specialists in the field of financial monitoring to study the data contained in the specified sources of information is studied and an information model of the process of studying decisions of arbitration courts is built. Based on the analysis of this model, a list of functions that the corresponding information resources intended for the automated analysis of arbitration court decisions should have is formed. An analysis of the existing functionality provided to analysts by well-known Internet resources intended for the automation of financial monitoring activities is carried out, and it is found that these Internet resources do not include tools for automatic analysis of arbitration case texts. In this regard, a conclusion is made about the relevance of the task of developing such a tool based on the use of machine learning methods, which are actively used today in the task of analyzing text information.

Keywords: *Rosfinmonitoring, 115-FZ, AML/CFT, analysis of arbitration court cases, machine learning.*

Введение

Федеральная служба по финансовому мониторингу Российской Феде-рации (Росфинмониторинг) является федеральным органом исполнительной власти РФ, к функциям которого отнесены: противодействие легализации (отмыванию) доходов, полученных преступным путём, финансирование терроризма, экстремистской деятельности и распространения оружия массового уничтожения, а также выработка государственной политики и нормативно-правовое регулирование в этой сфере, координация соответствующей деятельности федеральных органов исполнительной власти, других государственных органов и организаций, а также выполнение функций национального центра по оценке угроз национальной безопасности, возникающих в результате совершения операций (сделок) с денежными средствами или иным иму-ществом, и по выработке мер противодействия данным угрозам [1].

В соответствии со статьей 8 Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 07.08.2001 № 115-ФЗ [2]: «При наличии достаточных оснований, свидетельствующих о том, что операция, сделка связаны с легализацией (отмыванием) доходов, полученных преступным путем, или с финансированием терроризма, или с иным уголовно наказуемым деянием, уполномоченный орган[1] направляет соответствующие информацию и материалы в правоохранительные органы в соответствии с их компетенцией, установленной Уголовно-процессуальным кодексом Российской Федерации и Федеральным законом от 12 августа 1995 года № 144-ФЗ [3] «Об оперативно-розыскной деятельности», или налоговые органы по запросу указанных органов либо по собственной инициативе».

Единый порядок информационного взаимодействия в области противодействия отмыванию денег (ПОД) и финансированию терроризма описан в «Инструкции по организации информационного взаимодействия в сфере противодействия легализации (отмыванию) денежных средств или иного имущества, полученных преступным путем» утверждена приказом Генеральной прокуратуры Российской Федерации, Росфинмониторинга, Министерства внутренних дел Российской Федерации (МВД России), Федеральной службы безопасности Российской Федерации (ФСБ России), Федеральной таможенной службы Российской Федерации (ФТС России), Следственного комитета Российской Федерации 21.08.2018 № 511/244/541/433/1313/80 [4].

В пункте 12.1 данной инструкции определены основные задачи информационного обмена, решаемые Росфинмониторингом на стадии выявления и проверки первичной информации о фактах легализации (отмывания) денежных средств или иного имущества, одной из которых является: «проверка информации, получаемой от организаций, осуществляющих операции (сделки) с денежными средствами или иным имуществом, и других лиц, в соответствии с действующим законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма и выявление операций (сделок), имеющих признаки связи с легализацией (отмыванием) денежных средств или иного имущества» [4, п. 12.1].

Таким образом, в процессе проверки и выявления операций (сделок), имеющих признаки связи с легализацией (отмыванием) денежных средств или иного имущества, должен проводиться поиск источников и анализ ин-формации, характеризующей соответствующие этапы движения денежных средств (контекст финансовых операций). В настоящее время важными источниками информации, в ходе анализ которой могут быть обнаружены признаки отмывания денег, являются арбитражные судебные дела, так как лица, совершающие противоправные действия, используют различные многочисленные схемы вывода финансовых средств [5–8], одной из которых являются мнимые сделки, легализуемые, именно, через решения арбитражных судов [9].

Напомним, что определение мнимой сделки в российском законода-тельстве дано в статье 170 Гражданского кодекса Российской Федерации (ГК РФ) [10]. Согласно пункту 1 этой статьи, мнимая сделка – «это сделка, совершенная лишь для вида, без намерения

[1] Уполномоченный орган - федеральный орган исполнительной власти, принимающий меры по противодействию легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения в соответствии с Федеральным законом "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" от 07.08.2001 N 115-ФЗ.

создать соответствующие ей правовые последствия» [10, ст. 170, п. 1]. Примером мнимой сделки является следующая ситуация: два юридических лица[2] резидент и нерезидент[3] договариваются о взыскании долга через третейские суды или заключение мировых соглашений. После получения судебного решения нерезидент обращается в Федеральную службу судебных приставов (ФССП) для его исполнения, и далее, после исполнения судебного решения, получает возможность легального вывода денежных средств на счёт в иностранном банке.

В этой связи, выявление фактов использования описанной противо-правной схемы отмывания денег является одной из актуальных задач финансового мониторинга.

В первой части статьи описывается процесс анализа арбитражного дела аналитиком Росфинониторинга, во второй части статьи описывается анализ существующих решений для автоматизации анализа арбитражных дел.

1 ПРОЦЕСС АНАЛИЗА ДЕЛА

Результаты интервьюирования сотрудников аналитического отдела Межрегионального управления Росфинмониторинга по Уральскому федеральному округу показали, что анализ арбитражных дел и проверка фактов отсутствия/наличия незаконных действий их участников реализуется выпол-нением следующей последовательности действий.

1. Изучение сути дела. Аналитик читает знакомится с материалами дела, чтобы понять обстоятельства спора, участников, суммы и суть требований. Особое внимание уделяется документам, которые могут быть связаны с финансовыми операциями. Также рассматривается решение по делу, если оно есть.

В процессе изучения сути дела аналитик выполняет следующую последовательность действий:

1. Поиск дела.
2. Определение участников процесса: истца, ответчика, третьих лиц, имеющих отношение к делу.
3. Изучение предмета спора (например, взыскание долга, оспаривание сделки, нарушение договора, суммы, сроки, основания).
4. Изучение решения суда (при наличии).
5. Анализ текста судебного дела в целях оценки рисков ОД/ФТ, в том числе, при наличии соответствующих программных инструментов с помо-щью методов анализа и машинного обучения

2. Проверка участников. Проверка финансовых историй физических и юридических лиц, участвующих в деле и поиск дополнительной информа-ции об участниках в базах данных (БД) Росфинмониторинга и других госу-дарственных органов [12–18], а также в средствах массовой информации.

3. Сопоставление обстоятельств дела и финансовых операций участников. Проверка сделок между сторонами на предмет экономической целесообразности и реальности экономических отношений на основе всей собранной информации. Выявление признаков дробления платежей, фиктивных транзакций или мнимых сделок (например, несоответствие объемов товаров и указанных сумм) и других незаконных финансовых операций на основе типологий [19–21], а также проводится проверка финансовых операций, подпадающих под операции подлежащие обязательному контролю со стороны уполномоченных служб [2, ст. 6].

---

[2] В соответствие с Федеральным законом «О валютном регулировании и валютном контроле» от 10.12.2003 № 173-ФЗ (последняя редакция) [11, ст. 1, п. 6] к резидентам РФ от-носятся:

а) физические лица, имеющие постоянное местожительство в Российской Федерации, в том числе временно находящиеся за пределами Российской Федерации;

б) юридические лица, созданные в соответствии с законодательством Российской Федера-ции, с местонахождением в Российской Федерации;

в) предприятия и организации, не являющиеся юридическими лицами, созданные в соответствии с законодательством Российской Федерации, с местонахождением в Россий-ской Федерации;

г) дипломатические и иные официальные представительства Российской Федерации, находящиеся за пределами Российской Федерации;

д) находящиеся за пределами Российской Федерации филиалы и представительства резидентов, указанных в подпунктах "б" и "в" настоящего пункта.

[3] В соответствие с 173 ФЗ [11, ст. 1, п.7] к нерезидентам относятся:

а) физические лица, имеющие постоянное местожительство за пределами Российской Федерации, в том числе временно находящиеся в Российской Федерации;

б) юридические лица, созданные в соответствии с законодательством иностранных государств, с местонахождением за пределами Российской Федерации;

в) предприятия и организации, не являющиеся юридическими лицами, созданные в соответствии с законодательством иностранных государств, с местонахождением за пределами Российской Федерации;

г) находящиеся в Российской Федерации иностранные дипломатические и иные официальные представительства, а также международные организации, их филиалы и представительства;

д) находящиеся в Российской Федерации филиалы и представительства нерезидентов, указанных в подпунктах "б" и "в" настоящего пункта.

4. Составление информационной справки. Аналитик формирует информационную справку с описанием выявленных признаков подозрительных операций и схем, обоснованием их потенциальной связи с противоправной деятельностью. При наличии достаточных оснований, свидетельствующих о том, что операция или сделка связаны с легализацией (отмыванием) денежных средств или иного имущества, или с финансированием терроризма, или с иным уголовно наказуемым деянием (далее, в соответствие со статьей 8 № 115-ФЗ) [2] (п. 21 инструкции «Инструкции по организации информационного взаимодействия в сфере противодействия легализации (отмыванию) денежных средств или иного имущества, полученных преступным путем» [4]), Росфинмониторинг направляет информацию в правоохранительные/надзорные органы для проведения последующего расследования (проверки) установленных признаков подозрительной деятельности.

В подпунктах пункта 22.2. [4] описаны сведения, которые должна содержать информационная справка, а именно:

22.2.1. О поводе для проведения финансового расследования: запрос правоохранительного органа, иное (в том числе, инициативное расследование на основе анализа и оценки рисков); о характере и об источнике поступления в Росфинмониторинг (его территориальные органы) информации о финансовых операциях и других сделках с денежными средствами или иным имуществом.

22.2.2. Об установочных данных, позволяющих идентифицировать юридических и физических лиц, совершающих (или совершавших) финансовые операции и другие сделки с денежными средствами или иным имуществом, возможно связанные с легализацией (отмыванием) денежных средств или иного имущества, их представителей и (или) выгодоприобретателей, бенефициарных владельцев.

22.2.3. О финансовых операциях (сделках), совершенных в рамках предикатных по отношению к легализации (отмыванию) денежных средств или иного имущества преступлений.

22.2.4. О периоде, общем количестве и суммах совершенных финансовых операций и других сделок с денежными средствами или иным имуществом с целью легализации (отмывания) денежных средств или иного имущества.

22.2.5. О выявленной схеме легализации (отмывания) денежных средств или иного имущества и признаках, свидетельствующих о том, что совершенные финансовые операции и другие сделки с денежными средствами или иным имуществом могут быть связаны с легализацией (отмыванием) денежных средств или иного имущества.

22.2.6. О денежных средствах, ценностях и об ином имуществе (включая сведения о местонахождении имущества), полученных лицами, указанными в подпункте 22.2.2 пункта 22 настоящей Инструкции, в результате совершения преступлений, предусмотренных статьями 174 и 174.1 УК РФ, связанных с ними предикатных преступлений, а также о доходах от этого имущества.

Таким образом, на 1 этапе алгоритма анализа арбитражных дел и проверки фактов отсутствия/наличия незаконных действий их участников собирается информация необходимая для пункта 22.2.2., на 2 этапе для пунктов 22.2.3., 22.2.4. на 3 этапе для пунктов 22.2.5., 22.2. Таким образом, обсуждаемая последовательность действий, прямо не прописанная в действующих нормативно-правовых актах, регламентирующих действия в сфере финансового мониторинга, согласуется с данными документами.

Для целей дальнейшего исследования представим обсуждаемую последовательность действий, выполняемых в ходе анализа арбитражных дел и проверки фактов отсутствия/наличия незаконных действий их участников в соответствие с методологией IDEF0 (рисунок 1–3).:

Рис. 1. Диаграмма A0

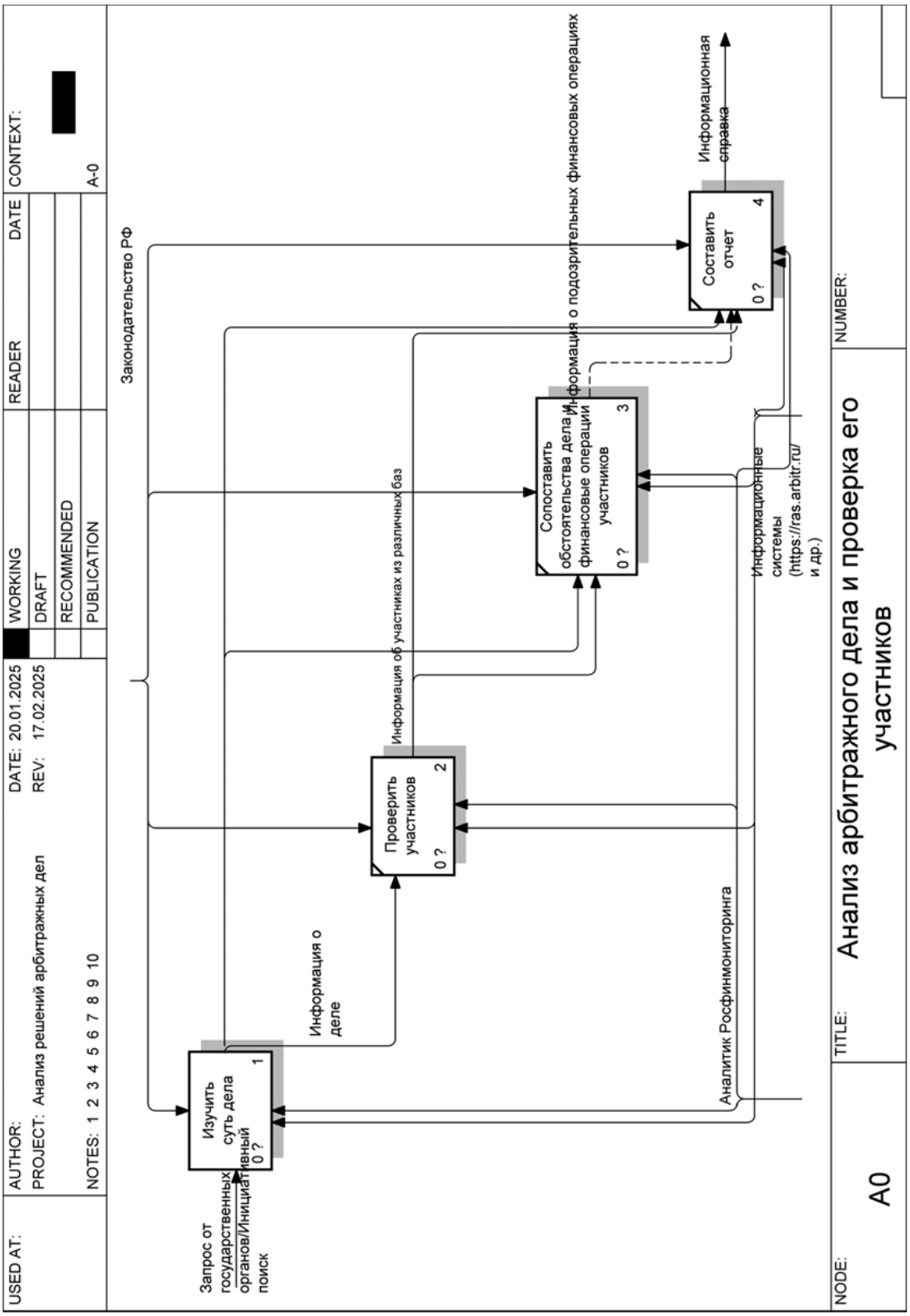

Рис. 2. Декомпозированная диаграмма A0

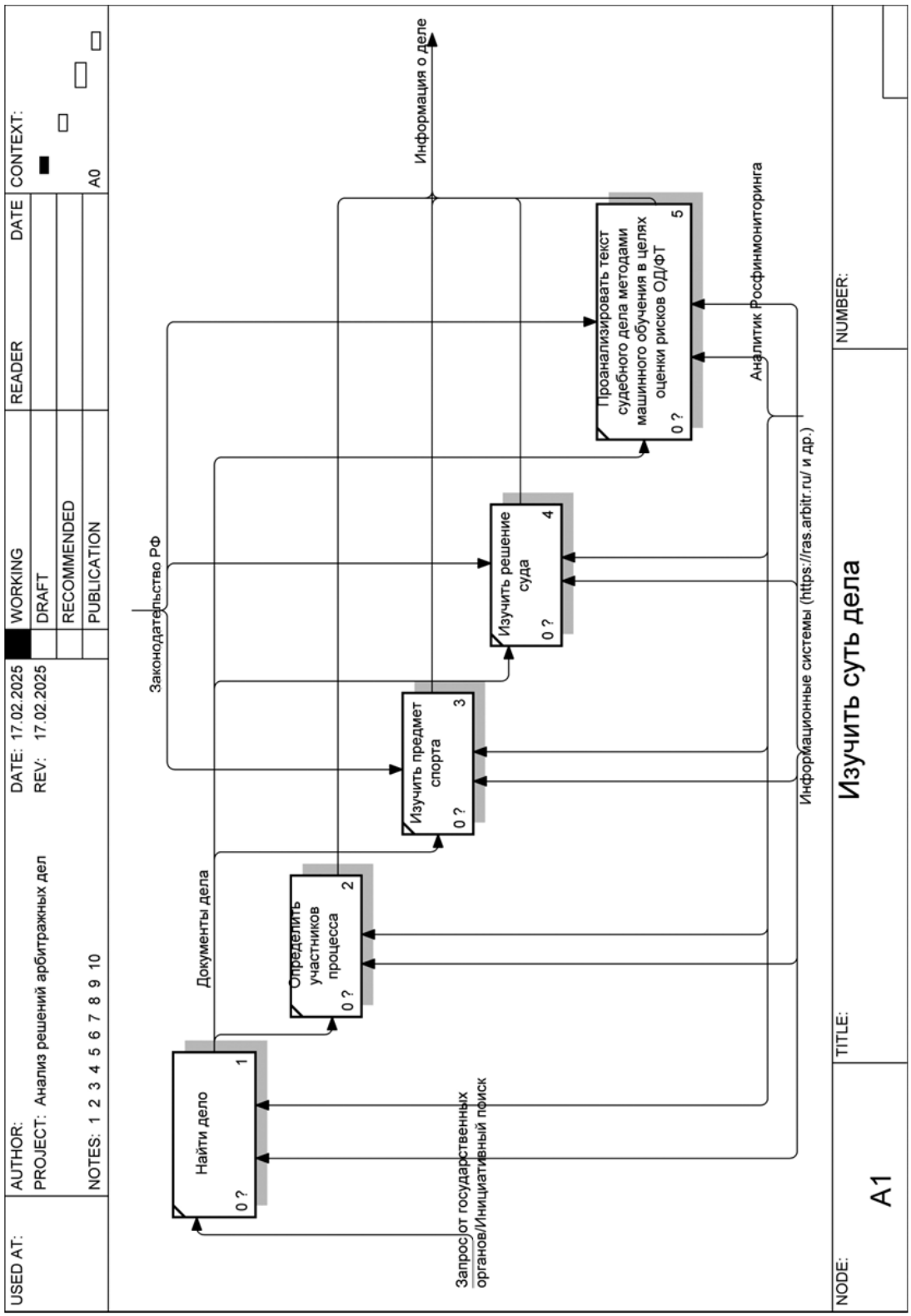

Рис. 3. Декомпозированная диаграмма A1

Из рисунков 1–3 видно, что выход блока «Изучить суть дела»: «Информация о деле» используется во всех следующих блоках процесса «Анализ арбитражного дела и проверка его участников» и поэтому является самым важным процессом для автоматизации при анализе решений арбитражных судов.

В этой связи был проведен в сети Интернет информационный поиск соответствующих ресурсов, результаты которого представлены в следующей части статьи.

2 АНАЛИЗ СУЩЕСТВУЮЩИХ РЕШЕНИЙ

По результатам проведенного поиска были обнаруженные следующие ресурсы, предназначенные для автоматизированного анализа арбитражных дел.

1. Интернет ресурс «Контур.Фокус» [22].
2. Интернет ресурс «СПАРК-Интерфакс» [23].
3. Интернет-ресурс «Casebook» [24].

Отметим, что сервис анализ арбитражных дел, на данных ресурсах является частью совокупностей инструментов для проведения комплексных проверок контрагентов. Скриншоты страниц сервисов, представляющих интерес для целей данного исследования представлены на рисунках 4–11.

Контур.Фокус

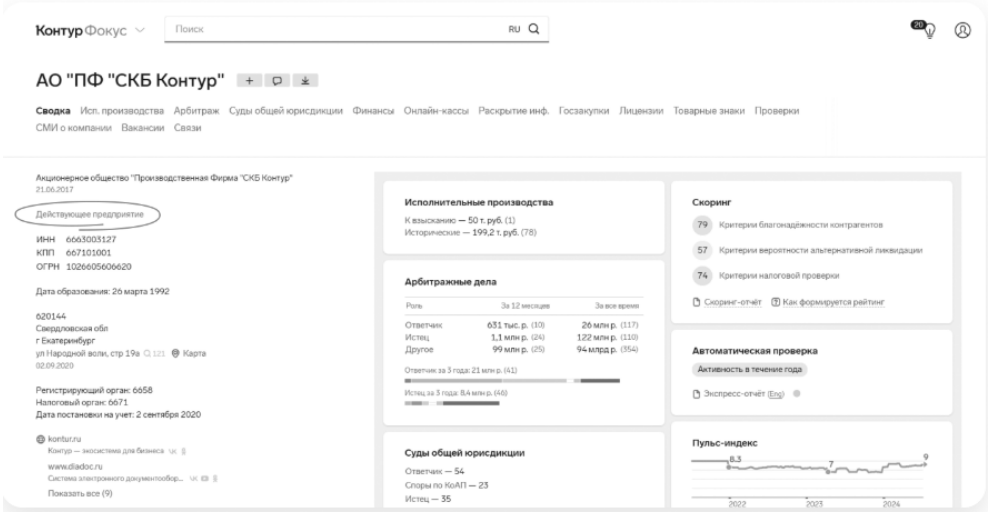

Рис. 4. Информация о юридических или физических лицах при проверке в сервисе Контур.Фокус [25]

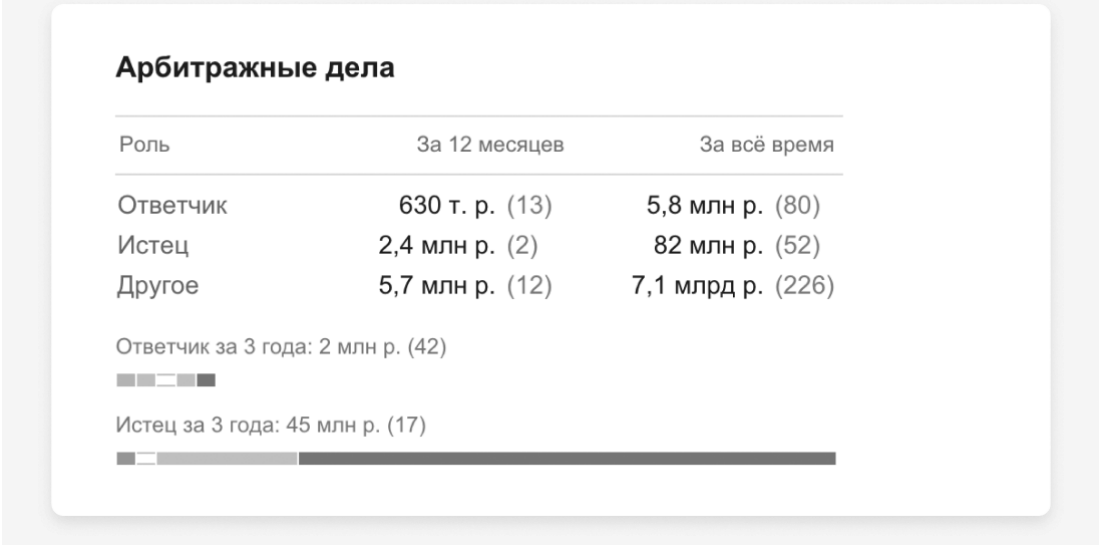

Рис. 5. Карточка по арбитражным делам юр. или физ. лица Контур.Фокус [26]

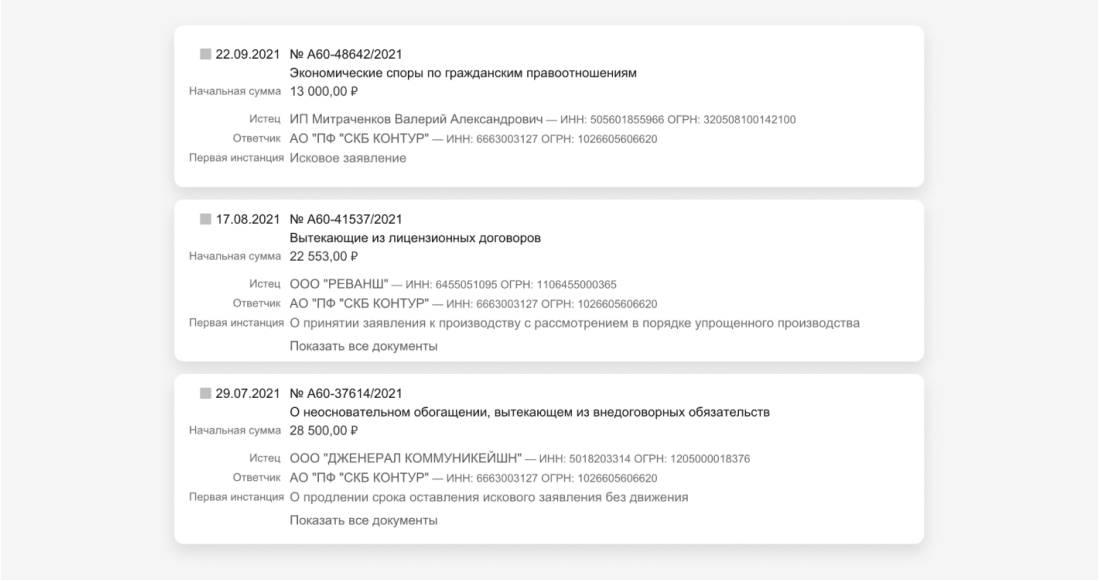

Рис. 6. Список арбитражных дел юр. или физ. лица [26]

СПАРК-Интерфакс

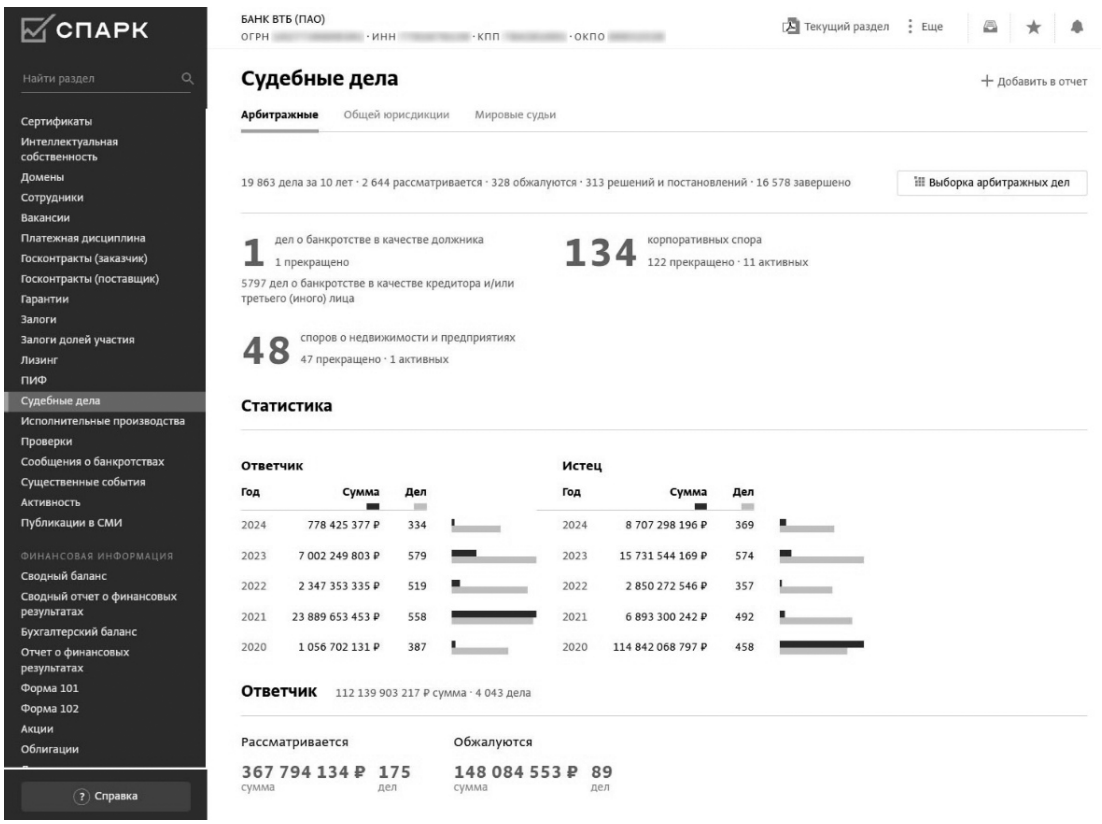

Рис. 7. Информация по арбитражным делам юр. или физ. лица в сервисе СПАРК-Интерфакс [23]

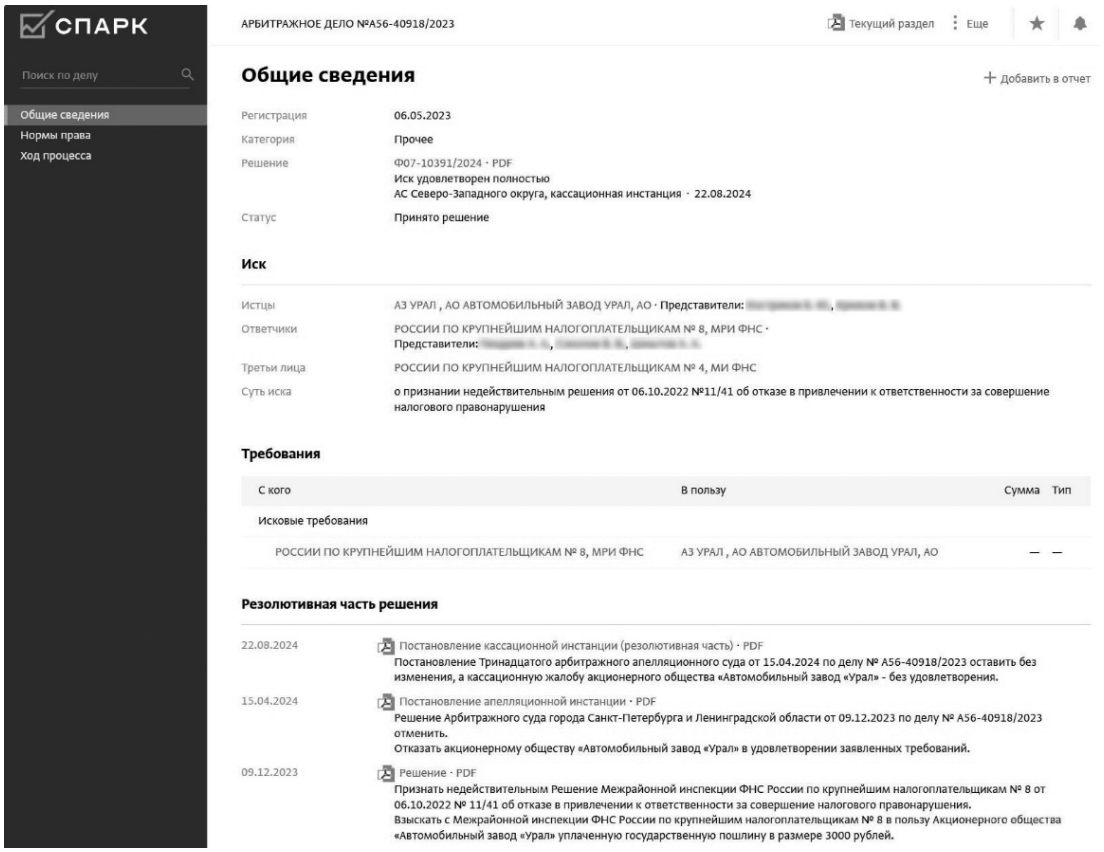

Рис. 8. Общие сведения об арбитражном деле СПАРК-Интерфакс [23]

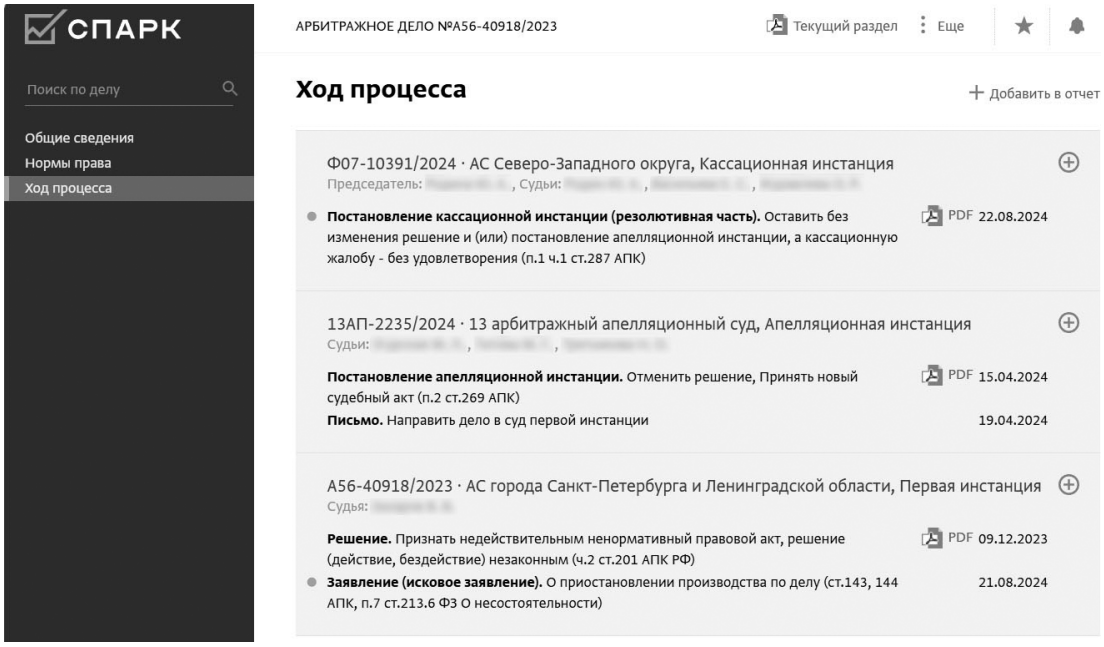

Рис. 9. Ход процесса арбитражного дела СПАРК-Интерфакс [23]

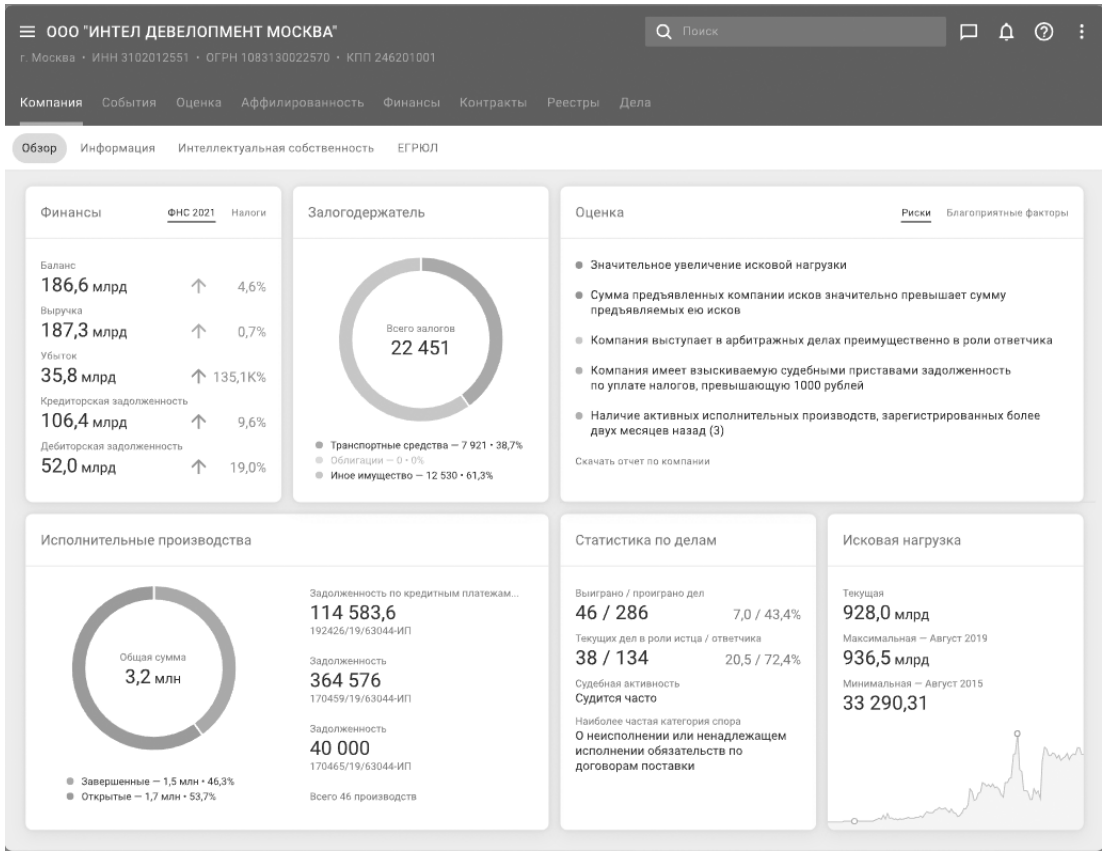

Рис. 10. Карточка юр. или физ. лица в сервисе Casebook [24]

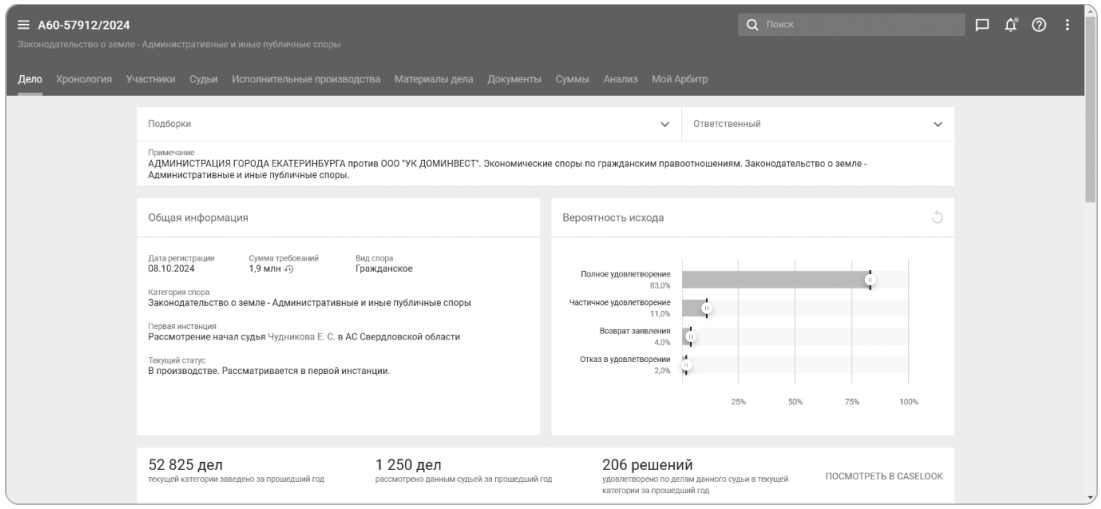

Рис. 11. Карточка арбитражного дела Casebook [27]

Таблица 1

Сравнение сервисов

Функция	**Контур. Фокус**	**СПАРК-Интерфакс**	**Casebook**
Поиск арбитражного дела	Да	Да	Да
Определение участников процесса	Да	Да	Да
Выделение предмета спора	Да	Да	Да
Возможность посмотреть решение суда	Да	Да	Да
Анализ текста судебного дела методами машинного обучения в целях оценки рисков ОД/ФТ	Нет	Нет	Нет
Проверка участников	Да	Да	Да

На основе использования представления алгоритма анализа арбитражных дел и проверки фактов отсутствия/наличия незаконных действий их участников в виде SADT-диаграмм (рисунок 1-3) был определен перечень требуемых характеристик сервисов для автоматизированного анализа решения арбитражных судов и проведено сравнение по данным критериям сервисов Контур.Фокус [22], СПАРК-Интерфакс [23], Casebook [24] друг с другом, результаты которого представлены в Таблице 1. Необходимая для этого информация была получена с официальных сайтов данных Интернет-серисов.

Из таблицы 1 видно, что ни один из популярных сегодня Интернет- сер-висов не предоставляет финансовому аналитику инструментов для анализа текстов судебных дел арбитражных судов методами машинного обучения в целях оценки рисков ОД/ФТ.

В этой связи, задача обоснования возможности создания программных инструментов для автоматизации поиска и анализа текстов судебных решений арбитражных судов, в том числе методами машинного обучения, в целях выявления признаков ОД/ФТ и оценивания их рисков является актуальной.

Заключение

Были описаны процесс анализа арбитражного дела аналитиком Росфин-мониторинга с целью поиска незаконных финансовых операций и анализ существующих решений для автоматизации части этого процесса.

В настоящий момент разрабатывается алгоритмическое и программное обеспечения для автоматизации процесса анализа текстов арбитражных дел методами машинного обучения.

Литература

1. Вопросы Федеральной службы по финансовому мониторингу (вместе с Положением о Федеральной службе по финансовому мониторингу) [Электронный ресурс]: Указ Президента РФ от 13.06.2012 N 808 в ред. от 26.12.2024. Доступ из справ. - правовой системы «КонсультантПлюс».

2. О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма [Электронный ресурс]: Федеральный закон от 07.08.2001 N 115-ФЗ в ред. от 28.12.2024. Доступ из справ.-правовой системы «КонсультантПлюс».

3. Об оперативно-розыскной деятельности [Электронный ресурс]: Феде-ральный закон от 12.08.1995 N 144-ФЗ в ред. от 29.12.2022. Доступ из справ.-правовой системы «КонсультантПлюс».

4. Об утверждении Инструкции по организации информационного взаимодействия в сфере противодействия легализации (отмыванию) денежных средств или иного имущества, полученных преступным путем [Электронный ресурс]: Приказ Генпрокуратуры России N 511, Росфинмониторинга N 244, МВД России N 541, ФСБ России N 433, ФТС России N 1313, СК России N 80 от 21.08.2018. Доступ из справ. - правовой системы «КонсультантПлюс».

5. Росфинмониторинг выявил новые схемы вывода средств с участием физлиц [Электронный ресурс] / Российская газета: сайт. URL: https://rg.ru/2024/05/17/rosfinmonitoring-vyiavil-novye-shemy-vyvoda-sredstv-s-uchastiem-fizlic.html (дата обращения: 03.02.2025).

6. Налог за доходы: в России обнаружили новую схему обналичивания денег [Электронный ресурс] / Федеральная служба по финансовому монито-рингу: официальный сайт. URL: https://www.fedsfm.ru/mediaaboutus/4996 (дата обращения: 03.02.2025).

7. Центробанк выявил схему по отмыванию денег с помощью инвестиционных монет [Электронный ресурс] / Федеральная служба по финансовому мониторингу: официальный сайт. URL: https://www.fedsfm.ru/mediaaboutus/6306 (дата обращения: 03.02.2025).

8. В Росфинмониторинге рассказали о самой изощренной схеме мошенников [Электронный ресурс] / Федеральная служба по финансовому мониторингу: официальный сайт. URL: https://www.fedsfm.ru/mediaaboutus/7329 (дата обращения: 03.02.2025).

9. Обзор судебных актов по противодействию отмыванию доходов, полученных преступным путем [Электронный ресурс] / Агентство «ФКД консалт»: сайт. URL: https://fkdconsult.ru/obzor-sudebnyh-aktov-po-protivodejstviyu-legalizaczii-otmyvaniyu-dohodov-poluchennyh-prestupnym-putem (дата обращения: 03.02.2025).

10. Гражданский кодекс Российской Федерации (ГК РФ) [Электронный ресурс]: Федеральный закон от 30 ноября 1994 года N 51-ФЗ в ред. от 08.08.2024. Доступ из справ.- правовой системы «КонсультантПлюс».

11. О валютном регулировании и валютном контроле [Электронный ре-сурс]: Федеральный закон от 10.12.2003 N 173-ФЗ в ред. от 08.08.2024. Доступ из справ. - правовой системы «КонсультантПлюс».

12. Проверить статус налогоплательщика налога на профессиональный доход [Электронный ресурс] / Федеральная налоговая служба России: официальный сайт. URL: https://npd.nalog.ru/check-status/?utm_source=google.com&utm_medium=organic&utm_campaign=kdelu (дата обращения: 17.02.2025).

13. Банк данных исполнительных производств [Электронный ресурс] / Федеральная служба судебных приставов: официальный сайт. URL: https://fssp.gov.ru/iss/ip/ (дата обращения: 17.02.2025).

14. Реестр розыска по исполнительным производствам [Электронный ресурс] / Федеральная служба судебных приставов: официальный сайт. URL: https://fssp.gov.ru/iss/ip_search (дата обращения: 17.02.2025).

15. Единый федеральный реестр юридически значимых сведений о фактах деятельности юридических лиц, индивидуальных предпринимателей и иных субъектов экономической деятельности [Электронный ресурс]: официальный сайт. URL: https://fedresurs.ru/ (дата обращения: 17.02.2025).

16. Сведения из реестра недобросовестных поставщиков (подрядчиков, исполнителей) и реестра недобросовестных подрядных организаций [Элек-тронный ресурс] / Единая информационная система в сфере закупок: официальный сайт. URL: https://zakupki.gov.ru/epz/dishonestsupplier/search/results.html (дата обращения: 17.02.2025).

17. Прозрачный бизнес [Электронный ресурс] // Федеральная налоговая служба России: официальный сайт. URL: https://pb.nalog.ru/?utm_source=google.com&utm_medium=organic&utm_campaign=kdelu (дата обращения: 17.02.2025).

18. Предоставление сведений из ЕГРЮЛ/ЕГРИП в электронном виде [Электронный ресурс] / Федеральная налоговая служба России: официальный сайт. URL: https://egrul.nalog.ru/index.html?utm_source=google.com&utm_medium=organic&utm_campaign=kdelu (дата обращения: 17.02.2025).

19. Документы международных организаций [Электронный ресурс] / Международный учебно-методический центр финансового мониторинга: официальный сайт. URL: https://mumcfm.ru/mediateka/international (дата обращения: 17.02.2025).

20. Типологические отчеты ФАТФ [Электронный ресурс] / Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма (ЕАГ): официальный сайт. URL: https://eurasiangroup.org/ru/fatf-typology-reports (дата обращения: 17.02.2025).

21. Отчеты по типологическим исследованиям [Электронный ресурс] / Федеральная служба по финансовому мониторингу: официальный сайт. URL: https://www.fedsfm.ru/documents/international-fatf1/6401 (дата обращения: 17.02.2025).

22. Аналитика арбитражных дел [Электронный ресурс] / СКБ Контур: сайт. URL: https://focus.kontur.ru/site/capabilities/arbitration (дата обращения: 17.02.2025).

23. Арбитражные дела по ИНН организации: проверить судебные дела контрагента | Поиск по арбитражным делам и мониторинг по отдельным типам судебных разбирательств [Электронный ресурс] / Информационное агентство Интерфакс: сайт. URL: https://spark-interfax.ru/features/arbitration-proceedings (дата обращения: 17.02.2025).

24. Проверка контрагентов, поиск и мониторинг судебных дел: арбитражные дела, СОЮ [Электронный ресурс] / Право.ру: сайт. URL: https://casebook.ru/ (дата обращения: 17.02.2025).

25. Как проверить юрлицо, ИП и физлицо в Контур.Фокусе: инструкция [Электронный ресурс] / СКБ Контур: сайт. URL: https://focus.kontur.ru/site/news/52051-kak_proverit_yurlico_ip_i_fizlico (дата обращения: 17.02.2025).

26. Как проверка арбитражных дел в Фокусе поможет избежать рисков сотрудничества [Электронный ресурс] / СКБ Контур: сайт. URL: https://focus.kontur.ru/site/news/45031-analitika_arbitrazhnyh_del (дата обращения: 17.02.2025).

27. Карточка дела АС [Электронный ресурс] / Право.ру: сайт. URL: https://help.casebook.ru/?cat=36 (дата обращения: 17.02.2025).

References

1. Voprosy Federal'noj sluzhby po finansovomu monitoringu (vmeste s Polozheniem o Federal'noj sluzhbe po finansovomu monitoringu) [Jelektronnyj resurs]: Ukaz Prezidenta RF ot 13.06.2012 N 808 v red. ot 26.12.2024. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPljus».

2. O protivodejstvii legalizacii (otmyvaniju) dohodov, poluchennyh pre-stupnym putem, i finansirovaniju terrorizma [Jelektronnyj resurs]: Federal'nyj zakon ot 07.08.2001 N 115-FZ v red. ot 28.12.2024. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPljus».

3. Ob operativno-rozysknoj dejatel'nosti [Jelektronnyj resurs]: Fede-ral'nyj za-kon ot 12.08.1995 N 144-FZ v red. ot 29.12.2022. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPljus».

4. Ob utverzhdenii Instrukcii po organizacii informacionnogo vzaimo-dejstvija v sfere protivodejstvija legalizacii (otmyvaniju) denezhnyh sredstv ili inogo imushhestva, poluchennyh prestupnym putem [Jelektron-nyj resurs]: Prikaz Genprokuratury Rossii N 511, Rosfinmonitoringa N 244, MVD Rossii N 541, FSB Rossii N 433, FTS Rossii N 1313, SK Rossii N 80 ot 21.08.2018. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPljus».

5. Rosfinmonitoring vyjavil novye shemy vyvoda sredstv s uchastiem fiz-lic [Jelektronnyj resurs] / Rossijskaja gazeta: sajt. URL: https://rg.ru/2024/05/17/rosfinmonitoring-vyiavil-novye-shemy-vyvoda-sredstv-s-uchastiem-fizlic.html (data obrashhenija: 03.02.2025).

6. Nalog za dohody: v Rossii obnaruzhili novuju shemu obnalichivanija deneg [Jelektronnyj resurs] / Federal'naja sluzhba po finansovomu monitorin-gu : oficial'nyj sajt. URL: https://www.fedsfm.ru/mediaaboutus/4996 (da-ta obrashhenija: 03.02.2025).

7. Centrobank vyjavil shemu po otmyvaniju deneg s pomoshh'ju investicion-nyh monet [Jelektronnyj resurs] / Federal'naja sluzhba po finansovomu monitoringu : oficial'nyj sajt. URL: https://www.fedsfm.ru/mediaaboutus/6306 (data obrashhenija: 03.02.2025).

8. V Rosfinmonitoringe rasskazali o samoj izoshhrennoj sheme moshennikov [Jelektronnyj resurs] / Federal'naja sluzhba po finansovomu monitorin-gu: oficial'nyj sajt. URL: https://www.fedsfm.ru/mediaaboutus/7329 (da-ta obrashhenija: 03.02.2025).

9. Obzor sudebnyh aktov po protivodejstviju otmyvaniju dohodov, polu-chennyh prestupnym putem [Jelektronnyj resurs] / Agentstvo «FKD kon-salt»: sajt. URL: https://fkdconsult.ru/obzor-sudebnyh-aktov-po-protivodejstviyu-legalizaczii-otmyvaniyu-dohodov-poluchennyh-prestupnym-putem (data obrashhenija: 03.02.2025).

10. Grazhdanskij kodeks Rossijskoj Federacii (GK RF) [Jelektronnyj re-surs]: Federal'nyj zakon ot 30 nojabrja 1994 goda N 51-FZ v red. ot 08.08.2024. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPljus».

11. O valjutnom regulirovanii i valjutnom kontrole [Jelektronnyj resurs]: Fed-eral'nyj zakon ot 10.12.2003 N 173-FZ v red. ot 08.08.2024. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPljus».

12. Proverit' status nalogoplatel'shhika naloga na professional'nyj dohod [Jelektronnyj resurs] / Federal'naja nalogovaja sluzhba Rossii: ofici-al'nyj sajt. URL: https://npd.nalog.ru/check-status/?utm_source=google.com&utm_medium=organic&utm_campaign=kdelu (data obrashhenija: 17.02.2025).

13. Bank dannyh ispolnitel'nyh proizvodstv [Jelektronnyj resurs] / Fede-ral'naja sluzhba sudebnyh pristavov: oficial'nyj sajt. URL: https://fssp.gov.ru/iss/ip/ (data obrashhenija: 17.02.2025).

14. Reestr rozyska po ispolnitel'nym proizvodstvam [Jelektronnyj resurs] / Federal'naja sluzhba sudebnyh pristavov: oficial'nyj sajt. URL: https://fssp.gov.ru/iss/ip_search (data obrashhenija: 17.02.2025).

15. Edinyj federal'nyj reestr juridicheski znachimyh svedenij o faktah de-jatel'nosti juridicheskih lic, individual'nyh predprinimatelej i inyh sub#ektov jekonomicheskoj dejatel'nosti [Jelektronnyj resurs]: oficial'nyj sajt. URL: https://fedresurs.ru/ (data obrashhenija: 17.02.2025).

16. Svedenija iz reestra nedobrosovestnyh postavshhikov (podrjadchikov, is-polnitelej) i reestra nedobrosovestnyh podrjadnyh organizacij [Jelek-tronnyj resurs] / Edinaja informacionnaja sistema v sfere zakupok: ofi-cial'nyj sajt. URL: https://zakupki.gov.ru/epz/dishonestsupplier/search/results.html (data obrashhe-nija: 17.02.2025).

17. Prozrachnyj biznes [Jelektronnyj resurs] // Federal'naja nalogovaja sluzhba Rossii: oficial'nyj sajt. URL: https://pb.nalog.ru/?utm_source=google.com&utm_medium=organic&utm_campaign=kdelu (data obrashhenija: 17.02.2025).

18. Predostavlenie svedenij iz EGRJuL/EGRIP v jelektronnom vide [Jelek-tronnyj resurs] / Federal'naja nalogovaja sluzhba Rossii: oficial'nyj sajt. URL: https://egrul.nalog.ru/index.html?utm_source=google.com&utm_medium=organic&utm_campaign=kdelu (data obrashhenija: 17.02.2025).

19. Dokumenty mezhdunarodnyh organizacij [Jelektronnyj resurs] / Mezhdu-narodnyj uchebno-metodicheskij centr finansovogo monitoringa: oficial'nyj sajt. URL: https://mumcfm.ru/mediateka/international (data obrashhe-nija: 17.02.2025).

20. Tipologicheskie otchety FATF [Jelektronnyj resurs] / Evrazijskaja gruppa po protivodejstviju legalizacii prestupnyh dohodov i finansirovaniju terrorizma (EAG) : oficial'nyj sajt. URL: https://eurasiangroup.org/ru/fatf-typology-reports (data obrashhenija: 17.02.2025).

21. Otchety po tipologicheskim issledovanijam [Jelektronnyj resurs] / Federal'naja sluzhba po finansovomu monitoringu: oficial'nyj sajt. URL: https://www.fedsfm.ru/documents/international-fatf1/6401 (data obrashhenija: 17.02.2025).

22. Analitika arbitrazhnyh del [Jelektronnyj resurs] / SKB Kontur : sajt. URL: https://focus.kontur.ru/site/capabilities/arbitration (data obrashhenija: 17.02.2025).

23. Arbitrazhnye dela po INN organizacii: proverit' sudebnye dela kontragenta | Poisk po arbitrazhnym delam i monitoring po otdel'nym tipam sudebnyh razbiratel'stv [Jelektronnyj resurs] / Informacionnoe agentstvo Interfaks: sajt. URL: https://spark-interfax.ru/features/arbitration-proceedings (data obrashhenija: 17.02.2025).

24. Proverka kontragentov, poisk i monitoring sudebnyh del: arbitrazhnye dela, SOJu [Jelektronnyj resurs] / Pravo.ru: sajt. URL: https://casebook.ru/ (data obrashhenija: 17.02.2025).

25. Kak proverit' jurlico, IP i fizlico v Kontur.Fokuse: instrukcija [Jelektronnyj resurs] / SKB Kontur: sajt. URL: https://focus.kontur.ru/site/news/52051-kak_proverit_yurlico_ip_i_fizlico (da-ta obrashhenija: 17.02.2025).

26. Kak proverka arbitrazhnyh del v Fokuse pomozhet izbezhat' riskov sotrudnichestva [Jelektronnyj resurs] / SKB Kontur: sajt. URL: https://focus.kontur.ru/site/news/45031-analitika_arbitrazhnyh_del (data obrashhenija: 17.02.2025).

27. Kartochka dela AS [Jelektronnyj resurs] / Pravo.ru: sajt. URL: https://help.casebook.ru/?cat=36 (data obrashhenija: 17.02.2025).

АНДРЕЕВ Александр Михайлович, аспирант, ассистент Учебно-научного центра «Информационная безопасность» федерального государственного автономного образовательного учреждения высшего образования «Уральский федеральный университет им. первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 32. E-mail: a.m.andreev@urfu.ru

ПОРШНЕВ Сергей Владимирович, доктор технических наук, профессор Учебно-научного центра «Информационная безопасность» федерального государственного автономного образовательного учреждения высшего образования «Уральский федеральный университет им. первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 32. E-mail: s.v.porshnev@urfu.ru

ANDREEV Alexander Mikhailovich, postgraduate student, assistant of the Educational and Scientific Center «Information Security» of the Federal State Autonomous Educational Institution of Higher Education «Ural Federal University named after the first President of Russia B.N. Yeltsin». 620002, Yekaterinburg, st. Mira, 32. E-mail: a.m.andreev@urfu.ru

PORSHNEV Sergey Vladimirovich, Doctor of Technical Sciences, Professor of the Educational and Scientific Center «Information Security» of the Federal State Autonomous Educational Institution of Higher Education «Ural Federal University named after the first President of Russia B.N. Yeltsin». 620002, Yekaterinburg, st. Mira, 32. E-mail: s.v.porshnev@urfu.ru

УДК 004.056 Вестник УрФО № 1(55) / 2025, с. 21–28

Фатин А. Д.

DOI: 10.14529/secur250102

ПОСТРОЕНИЕ МОДЕЛИ АДАПТИВНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ: КЛАСТЕРИЗАЦИЯ, ИЗОЛЯЦИЯ И РЕКОНФИГУРАЦИЯ

Данная работа является продолжением исследования «Построение модели адаптивности киберфизических систем: функционирование и детектирование». Текущая часть фокусируется на решении задач кластеризации и изоляции узлов в киберфизических системах с помощью алгоритма пчелиной колонии (ABC) с последующей реконфигурацией. Используется адаптированный алгоритм ABC для определения оптимальной структуры кластеров, что позволяет минимизировать воздействие возможных аномалий на систему. Затем применяются полученные результаты кластеризации для эффективной изоляции аномальных узлов с последующей реконфигурацией системы для поддержания ее работоспособности.

Ключевые слова: *КФС, адаптивность, кластеризация, изоляция узлов, реконфигурация.*

Fatin A. D.

BUILDING A MODEL OF ADAPTABILITY OF CYBERPHYSICAL SYSTEMS: CLUSTERIZATION, ISOLATION AND RECONFIGURATION

This work is a continuation of the study "Building a model of adaptability of cyberphysical systems: functioning and detection." The current part focuses on solving clustering and node isolation problems in cyber-physical systems using the Bee Colony (ABC) algorithm followed by reconfiguration. An adapted ABC algorithm is used to determine the optimal cluster structure, which minimizes the impact of possible anomalies on the system. The obtained clustering results are then used to effectively isolate anomalous nodes, followed by reconfiguration of the system to maintain its functionality.

Keywords: *CPS, adaptivity, clustering, node isolation, reconfiguration.*

Введение

В ходе исследования [1] было принято к сведению, что адекватное реагирование на аномалии в киберфизических системах (согласно [2–5]) требует не только их точной диагностики, но и разработки стратегий, позволяющих минимизировать последствия данных событий. В первой части работы были рассмотрены методы обнаружения и анализа аномальных состояний. Теперь же, во второй части, акцент смещен на задачи кластеризации и изоляции узлов, которые являются критическими для поддержания целостности и стабильности системы при наличии потенциальных угроз.

В качестве алгоритмов кластеризации зачастую используются следующие подходы: CMNC [6], VCLANC [7], ANCA [8], метод кластеризации на основе пчелиной колонии (ABC) [9], CFCN [10] и др.

Алгоритм пчелиной колонии (ABC), изначально разработанный для решения задач оптимизации, в данном контексте адаптируется для определения наиболее устойчивой структуры кластеров узлов, что позволяет системе принимать взвешенные решения об изоляции отдельных узлов или групп узлов, которые могут представлять собой угрозу для функционирования всей сущности. При этом ключевым аспектом является сохранение работоспособности системы и минимизация влияния изоляционных мер на ее производительность.

В работе детально рассматривается процесс кластеризации, начиная с инициализации и заканчивая конвергенцией алгоритма, а также обсуждается, как каждый этап влияет на формирование оптимальных кластеров, аналогично работам [11–14]. Также вводится математическая модель, позволяющая количественно оценить качество разбиения и его пригодность для последующих действий по изоляции узлов. Особое внимание уделяется анализу взаимосвязи между результатами задачи кластеризации и последующей изоляцией узлов, поскольку правильное понимание этой взаимосвязи критично для разработки эффективной стратегии обеспечения безопасности системы.

В заключение введения подчеркивается, что предложенный подход не только повышает устойчивость системы к аномалиям, но и обеспечивает возможность ее адаптации и восстановления после изоляционных мер, что является неотъемлемой частью создания надежных и устойчивых киберфизических систем.

Решение задачи 3: кластеризация

Для решения задачи 3 [1] рекомендуется использовать ABC. Алгоритм пчелиной колонии (ABC) является методом оптимизации, который имитирует поведение пчел при поиске источников пищи. Для кластеризации системы адаптируем ABC для идентификации групп узлов, которые могут быть изолированы с минимальными потерями для системы.

Взаимосвязь решения задачи 2 с задачей 3

Алгоритм пчелиной колонии для решения этой задачи будет итеративно обновлять разбиение C и центроиды μ_k через процесс, имитирующий поведение пчел при поиске пищи:

1. Инициализация

Случайным образом производится распределение узлов по кластерам для начального приближения центроидов.

2. Разведка

«Пчелы-разведчики» исследуют пространство решений, предлагая новые разбиения.

3. Вербовка и эксплуатация

«Пчелы-рабочие» сосредотачиваются на наиболее перспективных решениях, улучшая их и уточняя центроиды.

4. Оценка

Расчет качества каждого разбиения с использованием целевой функции.

5. Фаза обновления

Удаление менее успешных решений и замена их новыми, генерируемыми «пчелами-разведчиками».

6. Конвергенция (сходимость)

Итерирование до тех пор, пока не будет достигнут критерий остановки (например, заданное количество итераций или достижение определенного уровня качества разбиения).

Данный процесс позволяет адаптивно исследовать пространство решений и находить оптимальное или близкое к оптимальному разбиение множества узлов на кластеры с учетом аномальных узлов.

Математическая модель

Пусть X — множество векторов состояний узлов системы, а A — множество индикаторов аномалий, полученных из задачи 2. Тогда задача кластеризации может быть сформулирована как оптимизационная проблема: найти такое разбиение C множества узлов X,

которое минимизирует функцию потерь L, учитывая аномальность некоторых узлов.

Целевая функция:

Минимизировать функцию потерь L, которая может включать внутрикластерное расстояние и, возможно, штраф за включение аномальных узлов в кластеры:

$$\mathrm{L(C)} = \sum_{\mathrm{k=1}}^{\mathrm{K}} \sum_{\mathrm{x_i} \in \mathrm{C_k}} \mathrm{d(x_i, \mu_k)} + \lambda \sum_{\mathrm{x_i} \in \mathrm{A}} \phi(\mathrm{x_i, C}), \quad (1)$$

где:

C — $C = \{C_1, C_1, \ldots, C_K\}$ — разбиение множества X на K кластеров,

C_k — узлы в кластере k,

x_i — вектор состояния узла i,

μ_k — центроид кластера C_k,

d — функция расстояния между вектором состояния узла x_i и центроидом кластера μ_k (например, евклидово расстояние),

λ — (коэффициент) параметр регуляризации, который контролирует влияние аномальных узлов на целевую функцию,

ϕ — функция штрафа за аномалии,

A — A=a1,a2,…,an представляет собой множество аномалий, где ai является индикатором (например, бинарным значением), который указывает, является ли i-й узел аномальным или нет,

K — количество кластеров, на которое нужно разделить множество X.

Ограничения кластеризации:

Каждый узел должен принадлежать ровно одному кластеру:

$$\forall i, \exists! \, k : x_i \in C_k, \quad (2)$$

и количество кластеров K может быть задано заранее или определено в процессе.

Для упрощения изменим вышеприведенную формулу целевой функции на следующую:

$$min_{(C,\mu_k)} \sum_{k=1}^{K} \sum_{x_i \in C_k} d(x_i, \mu_k) + \lambda \sum_{i=1}^{n} a_i \cdot \psi(x_i, C), \quad (3)$$

Решение задачи 4: изоляция узлов

Для решения задачи 4 будем использовать результаты задачи 3, чтобы определить, какие узлы следует изолировать для минимизации влияния аномалий на систему. Подход основан на стремлении к изоляции только тех узлов, которые являются источниками аномалий, и таким образом, чтобы минимизировать воздействие на функционирование системы.

Процесс оптимизации будет происходить по следующему алгоритму:

1. Инициализация переменных и установление начальных значений весов и коэффициентов.

2. Вычисление целевой функции I для текущего набора изолированных узлов.

3. Применение методов оптимизации для нахождения оптимального набора узлов для изоляции, удовлетворяющего ограничениям и минимизирующего целевую функцию.

4. Повторение шагов 2 и 3 до достижения критерия остановки (например, отсутствие улучшения целевой функции или достижение максимального количества итераций).

Ограничения:

1. Каждый узел может находиться лишь в одном состоянии изоляции:

$$\forall i, \gamma_i \in 0,1. \quad (4)$$

2. Изоляция узла возможна только если он аномален:

$$\forall i, \gamma_i = 1 \Rightarrow x_i \text{ может быть изолирован.} \quad (5)$$

3. Необходимо учитывать взаимодействие узлов внутри кластеров и между кластерами, чтобы минимизировать воздействие изоляции на систему.

Математическая модель

Целевая функция:

Минимизировать функцию воздействия изоляции I, которая учитывает потери функциональности системы из-за изоляции узлов и возможные штрафы за нарушение целостности кластеров:

$$\min_{\mathrm{I}} \left(\sum_{\mathrm{i} \in \mathrm{I}} \mathrm{w_i} \cdot \gamma_\mathrm{i} + \delta \sum_{\mathrm{k=1}}^{\mathrm{K}} \eta(\mathrm{C_k, I}) \right), \quad (6)$$

где:

w_i — вес узла i, отражающий его важность для системы.

γ_i — индикатор аномалии узла i, полученный из задачи 2 (1, если узел аномален, и 0 в противном случае).

δ — коэффициент, который контролирует влияние нарушения целостности кластеров на целевую функцию.

$\eta(C_k,I)$ — функция штрафа за изоляцию узлов в кластере C_k, которая увеличивается, если узлы из одного кластера изолированы несоразмерно.

На выходе решения получаем набор узлов для изоляции, который минимизирует воздействие на систему и учитывает аномальность узлов и целостность кластеров.

Решение задачи 5: реконфигурация

После изоляции узлов система должна быть реконфигурирована, чтобы продолжить функционировать без изолированных узлов.

Шаги решения:

1. Произвести переоценку сетевой топологии без изолированных узлов.

2. Определить новые пути и связи для маршрутизации задач и потоков данных.

3. Распределить ресурсы и нагрузку между оставшимися узлами.

4. Применить изменения в системе и проверить ее работоспособность.

Для решения задачи реконфигурации системы можно воспользоваться системой оркестрации контейнеров, таких как, например, Kubernetes (k8s). В последних, зачастую, существуют механизмы автоматического масштабирования, самовосстановления и управления конфигурацией.

Математическая модель

Пусть S будет множеством всех узлов в системе, а I – множеством изолированных узлов после решения задачи 4 (изоляция узлов). Тогда S'=S\I представляет собой множество узлов, оставшихся после изоляции.

1. Оценка новой топологии:

Определить новую матрицу связности C' для S', где каждый элемент c'ij указывает на наличие связи между узлами i и j в новой топологии.

2. Развертывание копий изолированных узлов:

Для каждого изолированного узла $i \in I$, найти подходящий ресурс в оркестраторе для развертывания его незараженной копии. Пусть R будет множеством всех доступных ресурсов в кластере оркестратора, тогда функция развертывания может быть описана как:

$$\text{Deploy: } I \times R \rightarrow S'', \tag{7}$$

где S'' – множество новых узлов, которые заменяют изолированные.

3. Распределение нагрузки:

Необходимо перераспределить нагрузку и задачи изолированных узлов на их новые копии. Пусть L будет функцией, которая отображает нагрузку li от изолированного узла i к новому узлу j:

$$L: I \times S'' \rightarrow R^+, \tag{8}$$

где R^+ – множество положительных вещественных чисел, представляющих нагрузку.

4. Обновление конфигурации:

Далее необходимо выполнить конфигурацию системы для отражения изменений в топологии и нагрузке. Для каждого нового узла $j \in S''$, следует обновить конфигурационные файлы Kj в оркестраторе:

$$Kj = \text{UpdateConfig}(j, C', L). \tag{9}$$

5. Применение изменений:

Применить изменения в оркестраторе, чтобы активировать новую конфигурацию:

$$\text{ApplyChanges}(Kj), \tag{10}$$

где ApplyChanges – процедура, которая запускает или обновляет поды, сервисы и другие ресурсы в оркестраторе согласно новой конфигурации.

6. Итоговая система:

После реконфигурации Sfinal будет объединением оставшихся и новых узлов:

$$\text{Sfinal} = S' \cup S''. \tag{11}$$

Улучшение модели в контексте применения нейронных сетей

Определение количества входных нейронов и размерности многомерного временного ряда (тривиальный случай)

Чтобы определить количество входных узлов (нейронов) для нейронной сети, необходимо знать размерность вектора X(t), который используется как входные данные для нейронной сети. Размерность этого вектора определяется количеством параметров в векторе состояния узла xi(t) и количеством параметров в векторе связности ci(t), умноженным на количество узлов N в системе.

Если предположить (рассматривая тривиальный случай с однотипными устройства), что каждый вектор состояния узла xi(t) имеет размерность p, а вектор связности ci(t) имеет размерность q (которая может быть равна N, если мы рассматриваем связь каждого узла со всеми остальными

узлами в сети), то объединенный вектор для одного узла $zi(t)$ будет иметь размерность $p+q$.

Таким образом, общее количество входных узлов для нейронной сети, соответствующее многомерному временному ряду $X(t)$, будет равно:

$$(\text{Количество входных узлов} = N\times(p+q), \quad (12)$$

где:

N – количество узлов в системе,

p – количество параметров состояния каждого узла,

q – количество параметров связности каждого узла (часто равно N, но может быть меньше, если сеть разреженная).

Данное число будет равно количеству входных нейронов, которые должны быть в первом слое нейронной сети, чтобы она могла обрабатывать входные данные, представленные в виде многомерного временного ряда $X(t)$.

Определение количества входных нейронов и размерности многомерного временного ряда (общий случай)

Однако, стоит отметить тот факт, что в общем случае размерность вектора состояния узла $xi(t)$ и размерность вектора связности $ci(t)$ могут быть для каждого узла произвольными.

Если размерность вектора состояния узла $xi(t)$ и размерность вектора связности $ci(t)$ могут быть разными для каждого (или некоторого количества) узла/узлов, то для определения количества входных узлов (нейронов) для нейронной сети потребуется слегка изменить подход.

Для каждого узла vi необходимо определить размерность вектора состояния pi и размерность вектора связности qi.

Просуммируем размерности векторов состояния и связности для всех узлов, чтобы получить общее количество параметров для всей системы. Таким образом формула «Количество входных узлов» выше будет иметь вид:

$$(\text{Количество входных узлов} = \sum_{i=1}^{N}(pi + qi), \quad (13)$$

где:

N – общее количество узлов в системе,

pi – размерность вектора состояния узла vi,

qi – размерность вектора связности узла vi.

Определение количества входных нейронов и размерности многомерного временного ряда (практический случай)

На практике, конечно, конфигурация части узлов будет повторяться, а значит, формула «Количество входных узлов» выше будет иметь следующий вид:

$$(\text{Количество входных узлов} = \sum_{i=1}^{M}(pi + qi)fi, \quad (14)$$

где:

M – количество семейств узлов, где каждое семейство включает в себя одинаковые типы узлов.

fi – количество узлов в i-м семействе.

pi и qi – размерности векторов, характерные для семейства fi.

Это общее количество параметров будет равно количеству входных нейронов, необходимых для первого слоя нейронной сети.

Для наглядности рассмотрим следующий пример.

Предположим, имеется система из трех узлов, где:

Семейство 1 имеет вектор состояния размерности = 4, вектор связности размерности = 2 и 3 узла.

Семейство 2 имеет вектор состояния размерности = 3, вектор связности размерности = 3 и 2 узла.

Семейство 3 имеет вектор состояния размерности = 5, вектор связности размерности = 4 и 5 узлов.

Тогда общее количество входных нейронов будет:

Количество входных узлов = $(4+2)\cdot3+$ $+(3+3)\cdot2+(5+4)\cdot5=75$

Таким образом, первый слой нейронной сети должен иметь 75 входных нейронов.

Также стоит отметить, что при работе с нейронными сетями и многомерными временными рядами, где размерности могут варьироваться, часто используются архитектуры, способные обрабатывать переменные размерности входных данных, такие как рекуррентные нейронные сети (RNN) или трансформеры, которые могут обрабатывать последовательности переменной длины. В таких случаях может потребоваться использо-

вать дополнительные техники предобработки данных, такие как padding (в данном случае дополнение нулями) или attention mechanisms, которые позволяют модели определять важность различных частей входных данных.

Использование параллельных нейронных сетей

Использование отдельной нейронной сети для каждого типа узлов может быть эффективным подходом, особенно если узлы различаются по своим функциям, характеристикам или типам данных.

Преимущества данного решения:

1. Специализация:

Каждая нейронная сеть может специализироваться на обработке данных определенного типа узлов, что позволяет более точно настраивать параметры и структуру сети под конкретные особенности данных.

2. Упрощение архитектуры:

Архитектура каждой нейронной сети может быть упрощена, поскольку она будет обрабатывать более однородный набор данных, что может снизить сложность модели и ускорить обучение.

3. Параллелизм:

Отдельные нейронные сети могут обучаться параллельно, что может существенно ускорить процесс обучения и оптимизации.

4. Модульность:

За счет реализации модульного подхода возможно упрощение тестирования, обновления, отладки, донастройки, а также масштабирования сетей, в т.ч. дополнительно упрощается введение нового класса устройств и модульное дообучение нужных сетей.

5. Гибкость управление ресурсами:

За счет возможности отдельного конфигурирования каждой из сетей появляется дополнительная вариативность по их профилированию, что позволяет упростить настройку сети по своему конечному назначению и, соответственно, агрегировать сети по требованиям к вычислительным ресурсам в отдельные кластеры.

Недостатки данного решения:

1. Усложнение интеграция:

При обработке данных нейронными сетями, выполняемой параллельно, следует учесть потенциальную возможность либо рассинхронизации выходных данных (при использовании разных моделей или различных весов в одинаковых моделях), либо заложить дополнительные ресурсы на дублирование работы или резервный ввод временных ресурсов системы в момент простоя нейронных сетей при дообучении одной из сетей и последующем дублировании их на старые модули.

2. Усложнение управления и мониторинга:

В случае работы последовательных моделей, вывод в которых напрямую используется в качестве ввода на следующем этапе вычислений, могут возникнуть проблемы при согласовании управления данными, вследствие чего могут потребоваться дополнительные средства мониторинга.

Использование отдельных нейронных сетей, работающих в параллельном или смешанном режиме, для разных типов узлов сети может иметь место, если это действительно улучшает эффективность работы системы и/или упрощает процесс обучения или обновления модели(ей). Однако стоит учитывать тот факт, что при разделении нейронных сетей на отдельные несвязанные сервисы возрастает и риск потери косвенных связей, так как. финальная сеть, агрегирующая данные, полученные из параллельных источников, может не уметь восстанавливать косвенные связи, а сами параллельные нейронные сети могут терять часть косвенных связей за счет неполной обработки данных.

Исходя из вышесказанного рекомендуется (при наличии мощностей) остановиться на монолитной нейронной сети для сохранения должного уровня связности данных и приемлемого уровня производительности системы.

Вывод

В работе были подробно расписаны математические модели, включающие в себя решения частных задач кластеризации компьютерных сетей, изоляции аномальный узлов и реконфигурации целевой киберфизической системы. Данные задачи являются логическим продолжением задач описания и детектирования аномалий, представленных в предыдущей работы, и суммарно представляют собой задачу адаптации киберфизических систем.

Конечным результатом выполненной работы является полноценная математическая модель, описывающая весь процесс адаптивности киберфизической системы в рамках ее функционирования в условиях возможного возникновения аномалий.

Литература

1. Фатин А.Д. Построение модели адаптивности киберфизических систем: функционирование и детектирование / А.Д. Фатин // Вопросы кибербезопасности. – 2024. – № 2 (60). – С. 36-43. DOI: 10.21681/2311-3456-2024-2-36-43

2. Zegzhda D., Lavrova D., Poltavtseva M. Multifractal security analysis of cyberphysical systems // Nonlinear phenomena in complex systems. – 2019. – Vol. 22. – Issue 2. – pp. 196–204.

3. Application model of modern artificial neural network methods for the analysis of information systems security / Demidov R.A., Pechenkin A.I., Zegzhda P.D., Kalinin M.O. // Automatic Control and Computer Sciences. – 2018. – Vol. 52. – № 8. – С. 965–970.

4. Kalinin M.O., Lavrova D.S., Yarmak A.V. Detection of threats in cyberphysical systems based on deep learning methods using multidimensional time series // Automatic Control and Computer Sciences. – 2018. – Vol. 52. – № 8. – pp. 912–917.

5. Zegzhda D.P., Vasil'ev Y.S., Poltavtseva M.A. Approaches to modeling the security of cyberphysical systems // Automatic control and computer sciences. – 2018. – Vol. 52. – Issue 8. – pp. 1000–1009.

6. Tensor Decomposition for Multilayer Networks Clustering / Zitai Chen et al. // Proceedings of the AAAI Conference on Artificial Intelligence. – 2019. – Vol. 33(01). – pp. 3371–3378. DOI: 10.1609/aaai.v33i01.33013371.

7. Variational Coembedding Learning for Attributed Network Clustering / Shuiqiao Yang et al. // arXiv – CS – Machine Learning (IF). – 2021. DOI: ar-xiv 2104.07295.

8. ANCA: Attributed Network Clustering Algorithm / Issam Falih et al. // COMPLEX NETWORKS2017: Complex Networks & Their Applications VI. – 2017. – pp. 241–252.

9. Saoud B. Networks clustering with bee colony. Artif Intell Rev 52. – 2019. – pp. 1297–1309. DOI: 10.1007/s10462-018-9657-8.

10. Ziruo J., Fuqiang Q. Network Clustering Algorithm Based on Fast Detection of Central Node / Jia Ziruo, Qi Fuqiang // Scientific Programming. – 2022. – pp 1–5. DOI: 10.1155/2022/ 4905190.

11. Automatic security management of smart infrastructures using attack graph and risk analysis / Ivanov D., Kalinin M., Krundyshev V., Orel E. // Proceed-ings of the world conference on smart trends in systems, security and sustainability, WS42020. – 2020. – pp. 295–300.

12. Krundyshev V., Kalinin M. Hybrid neural network frame work for detection of cyberattacks at smart infrastructures // ACM International Conference Proceeding Series. Proceedings of the 12th International Conference on Security of Information and Networks, SIN2019. – 2019. – pp. 3357623.

13. Полтавцева М.А. Адаптивный мониторинг информационной безопасности / М. А. Полтавцева. – СПб., 2021. – 166 с.

14. Савин И.В. Технология кластеризации для обеспечения отказоустойчивости / И. В. Савин // Известия Тульского государственного университета. Технические науки. – 2019. – № 3. – С. 191–194.

References

1. Fatin A.D. Postroyeniye modeli adaptivnosti kiberfizicheskikh sistem: funktsionirovaniye i detektirovaniye / A.D. Fatin // Voprosy kiber-bezopasnosti. – 2024. – № 2 (60). – S. 36-43. DOI: 10.21681/2311-3456-2024-2-36-43.

2. Zegzhda D., Lavrova D., Poltavtseva M. Multifractal security analysis of cy-berphysical systems // Nonlinear phenomena in complex systems. – 2019. – Vol. 22. – Issue 2. – pp. 196–204.

3. Application model of modern artificial neural network methods for the analysis of information systems security / Demidov R.A., Pechenkin A.I., Zegzhda P.D., Kalinin M.O. // Automatic Control and Computer Sciences. – 2018. – Vol. 52. – № 8. – С. 965–970.

4. Kalinin M.O., Lavrova D.S., Yarmak A.V. Detection of threats in cyberphysi-cal systems based on deep learning methods using multidimensional time series // Automatic Control and Computer Sciences. – 2018. – Vol. 52. – № 8. – pp. 912–917.

5. Zegzhda D.P., Vasil'ev Y.S., Poltavtseva M.A. Approaches to modeling the security of cyberphysical systems // Automatic control and computer sciences. – 2018. – Vol. 52. – Issue 8. – pp. 1000–1009.

6. Tensor Decomposition for Multilayer Networks Clustering / Zitai Chen et al. // Proceedings of the AAAI Conference on Artificial Intelligence. – 2019. – Vol. 33(01). – pp. 3371–3378. DOI: 10.1609/aaai.v33i01.33013371.

7. Variational Co-embedding Learning for Attributed Network Clustering / Shuiqiao Yang et al. // arXiv – CS – Machine Learning (IF). – 2021. DOI: ar-xiv 2104.07295.

8. ANCA: Attributed Network Clustering Algorithm / Issam Falih et al. // COM-PLEX NETWORKS2017: Complex Networks & Their Applications VI. – 2017. – pp. 241–252.

9. Saoud B. Networks clustering with bee colony. Artif Intell Rev 52. – 2019. – pp. 1297–1309. DOI: 10.1007/s10462-018-9657-8.

10. Ziruo J., Fuqiang Q. Network Clustering Algorithm Based on Fast Detection of Central Node / Jia Ziruo, Qi Fuqiang // Scientific Programming. – 2022. – pp 1–5. DOI: 10.1155/2022/ 4905190.

11. Automatic security management of smart infrastructures using attack graph and risk analysis / Ivanov D., Kalinin M., Krundyshev V., Orel E. // Proceedings of the world conference on smart trends in systems, security and sustainability, WS42020. – 2020. – pp. 295–300.

12. Krundyshev V., Kalinin M. Hybrid neural network frame work for detection of cyber-attacks at smart infrastructures // ACM International Conference Proceeding Series. Proceedings of the 12th International Conference on Security of Information and Networks, SIN2019. – 2019. – pp. 3357623.

13. Poltavtseva M.A. Adaptivnyy monitoring informatsionnoy bezopasnosti / M. A. Poltavtseva. – SPb., 2021. – 166 s.

14. Savin I.V. Tekhnologiya klasterizatsii dlya obespecheniya otkazoustoychivosti / I. V. Savin // Izvestiya Tul'skogo gosudarstvennogo univer-siteta. Tekhnicheskiye nauki. – 2019. – № 3. – S. 191–194.

Фатин Александр Денисович, аспирант, Санкт-Петербургский политехнический университет Петра Великого (СПбПУ). 195251, г. Санкт-Петербург, ул. Политехническая, д.29-Б. E-mail: sasha-fatin@mail.ru

Fatin Aleksandr Denisovich, postgraduate student, Peter the Great St. Petersburg Polytechnic University (SPbPU). 195251, St. Petersburg, Politekhnicheskaya St., 29-B. E-mail: sasha-fatin@mail.ru

УДК 004.056 + 669.1 Вестник УрФО № 1(55) / 2025, с. 29–36

Япаров Д. Д., Карманов Д. Е., Япарова Н. М. DOI: 10.14529/secur250103

МЕТОД ОБРАБОТКИ ИНФОРМАЦИИ ДЛЯ ПРОГНОЗИРОВАНИЯ СТЕПЕНИ ВОССТАНОВЛЕНИЯ МЕТАЛЛОВ НА ОСНОВЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ

Статья посвящена проблеме обеспечения достоверности информации о качестве продукции металлургических предприятий, связанных с производством металлов. Важным индикатором качества процесса получения металла из руды является степень металлизации. В работе предложен метод прогнозирования степени металлизации в процессе восстановления металла из различных соединений, основанный на использовании нейросетевых технологий. Целью работы является разработка алгоритмов, позволяющей с высокой точностью определять степень металлизации в зависимости от значений параметров процесса восстановления. Нейронная сеть, представленная в работе, включает обработку информации с помощью стратегий стохастического градиентного спуска, адаптивной оценки момента и обратного распространения ошибки. Предложенный комбинированный подход позволяет значительно повысить точность прогнозирования степени металлизации и обеспечить достоверность информации о реальной структуре металла, восстановленного из различных соединений. Достоверность информации, получаемой с помощью разработанной нейронной сети о степени металлизации, подтверждается результатами экспериментальных исследований.

Ключевые слова: *достоверность информации, нейронная сеть, обратное распространение ошибки, стохастический градиентный спуск, задача прогнозирования.*

INFORMATION PROCESSING METHOD FOR FORECASTING THE DEGREE OF METAL RECOVERY BASED ON NEURAL NETWORK TECHNOLOGIES

The article is devoted to the problem of ensuring the reliability of information on the quality of products manufactured by metallurgical enterprises. An important indicator of the quality of the process of obtaining metal from ore is the degree of metallization. The article proposes a method for predicting the degree of metallization in the process of metal recovery from various compounds, based on the use of neural network technologies. The purpose of the work is to develop algorithms that allow for highly accurate prediction of the degree of metallization based on the parameters of the recovery process. The neural network presented in the work includes information processing using stochastic gradient descent, adaptive moment estimation, and backpropagation strategies. The proposed combined approach can significantly improve the accuracy of predicting the degree of metallization and ensure the reliability of information on the real structure of metal recovered from various compounds. The reliability of the information obtained using the developed neural network on the degree of metallization is confirmed by the results of experimental studies

Keywords: information reliability, neural network, error backpropagation, stochastic gradient descent, forecasting issue..

Введение

При промышленном получении металла одним из ключевых индикаторов эффективности процесса восстановления металлов из руд или других источников является степень металлизации, показывающая объем металла, который была успешно переведен из исходного сырья в целевой продукт. Достоверность информации о степени восстановления способствует повышению точности оценки качества конечного продукта и обеспечивается созданием высокоточных методов, позволяющих распознать скрытую зависимость степени металлизации от значений параметров технологического процесса.

Создание и совершенствование нейросетевых технологий для решения прикладных задач, возникающих в промышленном производстве, относится к динамически развивающимся областям исследования [1-12]. Среди работ, связанных с использованием нейронных сетей для решения практических задач металлургии, отметим работу П.И. Аверина [13], в которой предложена нейронная сеть, созданная на основе радиальных базисных функций и позволяющая определить времени разрушения металлов на основе данных вейвлет-анализа импульсов акустической эмиссии. В работе А.С. Львова [14] предложен подход, позволяющий за счет выбора оптимального метода интерполяции повысить быстродействие нейронной сети, используемой для многопараметрического контроля состояния технологического процесса в металлургии. Разработке нейронной сети, оценивающей степень влияния химического состава металла на свойства стали и предназначенной для определения химического состава легирующего комплекса в процессе получения металлических сплавов посвящена работа И.Х. Тухватулина [15]. Отметим, что в настоящий момент остается нерешенной про-

блема определения по параметрам технологического процесса количества металла в конечном продукте, получаемого по завершении процесса выделения металлической компоненты из исходного материала. Таким образом, создание метода, направленного на выявление скрытой зависимости степени металлизации от значений параметров технологического процесса восстановления металла, относится к актуальному направлению исследований.

В данной статье предложена нейронная сеть, предназначенная для прогнозирования степени металлизации в зависимости от значений параметров технологического процесса восстановления металла из различных соединений. Основные преимущества предлагаемого метода заключается в том, что он позволяет определять степень металлизации с высокой точностью, используя для этого достаточно небольшой объем вычислительных ресурсов, и исключает трудоемкую процедуру аналитического выявления зависимости степени металлизации от значений параметров процесса восстановления, сопряженную с созданием многопараметрической математической модели и разработкой сложных вычислительных алгоритмов из процесса обработки информации.

Построение нейросетевой модели

Входными параметрами для нейросетевой модели процесса восстановления металла являются значения температуры, продолжительности процесса восстановления, состава восстановителя, массы образца. Исходные данные для обучающей и тестовой выборки формируются по оптическим изображениям поверхностей шлифов. Специфика рассматриваемой задачи восстановления металла заключается в малом объеме исходных данных, возникающей в силу сложности подготовки шлифов для экспериментального исследования. При малом объеме исходных данных возможна ситуация, когда обучающая и тестовая выборка окажутся неравномерно разделенными, и тогда точность нейронной сети, достигнутая на тестовых данных, будет существенно отличаться от точности обученной модели, что неизбежно приведет к искажению информации о точности обработки реальных данных с помощью этой сети. Для решения проблемы малого объема исходных данных в предлагаемой нейросетевой модели применяли аугментацию исходных данных.

Выборка изображений делится на 3 компонента в следующем соотношении: обучающая – 70 %, валидационная (проверочная) и тестовая – по 15 %. Обучающая выборка используется непосредственно в процессе обучения и является основной, проверочная часть датасета – для оптимизации гиперпараметров сети и исключения переобучения, тестовая – для оценки качества работы сети.

В предлагаемой нейронной сети функционирование нейрона k представлено следующими уравнениями:

$$u_k = \sum_{m=1}^{m} w_{km}\, x_m,$$
$$Y_k = \varphi(u_k + b_k),$$

где $x_1, x_2, \ldots x_m$ – значения входных параметров, $w_{k1}, w_{k2}, \ldots w_{km}$ – синаптические веса нейрона k; u_k– линейная комбинация входных воздействий; b_k – порог; $\varphi(.)$ – функция активации; Y_k – выходной сигнал нейрона.

Определения степени металлизации осуществляется на основе численных значений следующих параметров процесса восстановления металлов:

X_1 - процентная доля диоксид углерода в восстановителе;

X_2 - процентная доля монооксид углерода в восстановителе;

X_3 - процентная доля водорода в восстановителе;

X_4 - температура печи, в которой происходит восстановление металла;

X_5 - продолжительность процесса восстановления;

X_6 - масса образца до восстановления;

X_7 - масса образца после восстановления.

Параметры X_i , i=1,…,7 определяют входные данные для нейронной сети, а выходной параметр нейронной сети Y соответствует степени восстановления металла в целевом продукте. Разработка структуры искусственной нейронной сети осуществлялась на основе экспериментальных исследований. Программная реализация проводилось на языке программирования Python с применением программных платформ Keras, TensorFlow, Pandas, Scikit-Learn.

В процессе формирования структуры сети подбирались различные комбинации значений гиперпараметров, представленных в таблице 1. В общей сложности было рассмотрено 243 различных комбинаций.

Таблица 1

Гиперпараметры нейронной сети

Гиперпараметр	**Варианты значений гиперпараметров**		
Функция активации	Линейная функция	Сигмоида	ReLU
Количество эпох	5	10	35
Оптимизатор	Стохастический градиентный спуск (SGD), скорость обучения = 0.1	Адаптивная оценка момента (Adam), со скоростью обучения 0.1	Распространение среднеквадратичного значения (RMSProp) со скоростью обучения 0.1

Таким образом, для определения степени металлизации в зависимости от параметров процесса восстановления металлов предлагается многослойная нейронная сеть с последовательными слоями и полными связями между ними (модель Sequential или многослойный персептрон).

Результаты экспериментальных исследований

Формирования оптимальной структуры нейронной сети и определении набора гиперпараметров, позволяющего минимизировать значение функции потерь, осуществлялась на основе обработки оптических изображений различных проекций поверхности шлифов. В качестве функции потерь использовалась среднеквадратическая ошибка (MSE). Первый этап экспериментов связан с выбором наилучшей структуры нейронной сети. Результаты этого этапа представлены в табл. 2, 3 В табл. 2 приведены первые 7 комбинаций гиперпараметров. Комбинаций гиперпараметров с минимальными значениями функции потерь приведены в табл. 3.

В результате исследований сформирована следующая структура нейронной сети: входной слой состоит из 128 нейронов с функцией активации «ReLU», сеть включает один скрытый слой из 64 нейронов с функцией активации «ReLU», выходной слой состоит из одного нейрона с функцией активации «Linear». Оптимизатором сети является RMSProp.

Второй этап экспериментальных исследований предусматривал оценку качества работы нейронной сети, сформированной в результате первого этапа экспериментальных исследований. После проектирования и обучения искусственной нейронной сети с оптимальными параметрами на каждом слое установились веса. Основными показателями качества работы модели искусственной нейронной сети являются оценка точности работы нейронной сети и функция потерь. График функции потерь, используемой для расчета отклонений фактических результатов работы нейронной сети от ожидаемых при различном количестве эпох обучения, представлен на рисунке 1. Наименьшее значение функция

Таблица 2

Комбинаций гиперпараметров

№	**Слой 1**	**Слой 2**	**Слой3**	**Оптимизатор**	**Кол-во эпох**	**Функция потерь при проверке**
1	sigmoid	sigmoid	sigmoid	adam	5	0.99942
2	sigmoid	sigmoid	sigmoid	SGD	5	1.06434
3	sigmoid	sigmoid	sigmoid	RMSProp	5	0.99108
4	sigmoid	sigmoid	sigmoid	adam	20	0.75984
5	sigmoid	sigmoid	sigmoid	SGD	20	1.02163
6	sigmoid	sigmoid	sigmoid	RMSProp	20	0.76925
7	sigmoid	sigmoid	sigmoid	adam	35	0.68400

Таблица 3

Оптимальные значения гиперпараметров

№	Слой 1	Слой 2	Слой3	Оптимизатор	Кол-во эпох	Значения функции потерь
233	relu	relu	linear	RMSProp	35	0.01195
231	relu	relu	linear	adam	35	0.01203
150	linear	relu	linear	adam	35	0.01334
204	relu	linear	linear	adam	35	0.01603
147	linear	relu	linear	adam	20	0.01693
201	relu	linear	linear	adam	20	0.01800
228	relu	relu	linear	adam	20	0.02032

потерь достигала к 35 эпохе обучения. Таким образом, для получения наилучшей точности разработанной нейронной сети достаточно 35 эпох обучения.

Оценка точности работы нейронной сети производилась с помощью коэффициента детерминации, максимально возможное значение которого не превосходит единицы. Для разработанной нейронной сети значение коэффициента детерминации, полученное к 35 эпохе обучения, составило 0.9915, что свидетельствует о высокой точности результатов прогнозирования степени металлизации. На рис. 2 предоставлено соотношение числа верных предсказаний прогнозируемых значений к общему числу прогнозов: чем ближе точка расположена к прямой линии, тем точнее нейронная сеть обработала исходные данные и спрогнозировала степень металлизации.

Результаты эксперимента свидетельствуют о том, что построенная нейронная сеть обладает высокой точностью при малых значениях функции потерь и обеспечивает достоверность информации о степени металлизации в процессе восстановления металла из различных сред. Достоинство нейросетевого подхода заключается в отсутствии необходимости создавать сложные математические модели зависимости степени металлизации от параметров процесса восстановления.

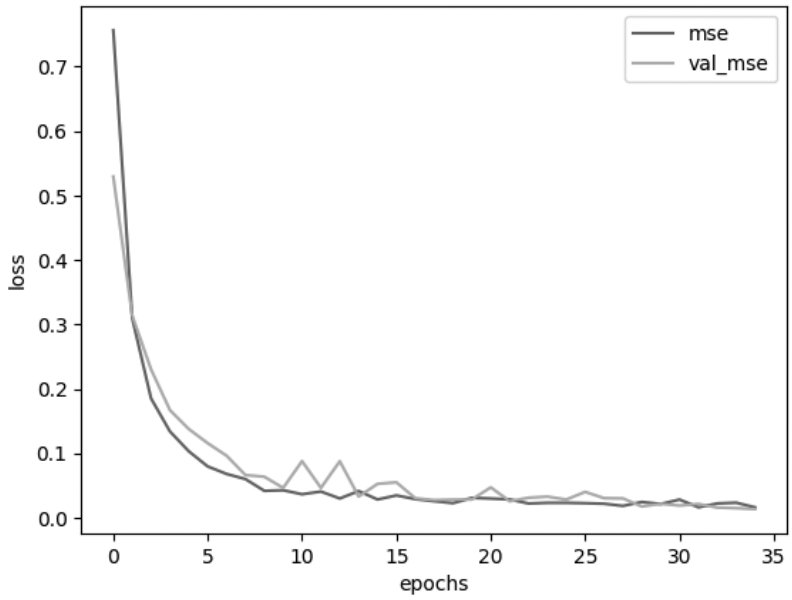

Рис. 1. График функции потерь

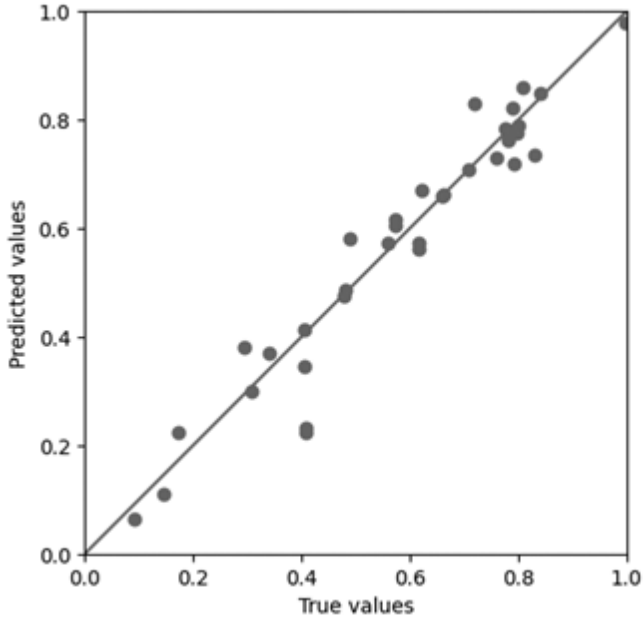

Рис. 2. График соотношения предсказанных значений от фактических

Заключение

В работе предложен метод обработки информации, созданный на основе нейросетевых технологий и предназначенный для прогнозирования степени металлизации по значениям параметров процесса восстановления металла. Обучение нейронной сети происходит с помощью стратегий исследования. Найдена оптимальная архитектура нейронной сети. Результаты экспериментальных исследований подтверждают высокую точность обработки информации с помощью предложенного метода и свидетельствуют о том, что нейронная сеть позволяет обеспечить достоверность информации о степени восстановления металлов из различных соединений.

Литература

1. Kohavi, R. A study of cross-validation and bootstrap for accuracy estimation and model selection / R. Kohavi // Proceedings of the Fourteenth International Joint Conference on Artificial Intelligence. San Mateo, 1995. – Vol. 2, № 12. – P. 1137–1143.

2. Hinton G. Dropout: A Simple Way to Prevent Neural Networks from Overfitting / G. Hinton et al. // Journal of Machine Learning Research. – 2014. – Vol. 15. – P. 1929–1958.

3. Krizhevsky, A. Imagenet classification with deep convolutional neural networks / A. Krizhevsky, I. Sutskever, G. Hinton // Proceedings of the 25th International Conference on Neural Information Processing Systems, NIPS. – 2012. – P. 1097–1105.

4. Diederik, P. Kihgma. Adam: A method for Stochastic Optimization, 2014 / Diederik P. Kihgma, Jimmy Ba // Proceedings of the 3rd International Conference on Learning Representations (ICLR).

5. Goodfellow I., Bengio Y., Courville A. Deep learning. Genet Program Evolvable Mach, 2018, vol. 19, pp. 305–307. DOI: 10.1007/s10710-017-9314-z.

6. Krizhevsky A., Sutskever I., Hinton G.E. ImageNet classification with deep convolutional neural networks. Communications of the ACM, 2017, vol. 60, no. 6, pp. 84–90. DOI: 10.1145/3065386.

7. Япаров, Д. Д. оценка метода восстановления входного сигнала по зашумленным данным / Д. Д. Япаров // Вестник УрФО. Безопасность в информационной сфере. – 2022. – № 4(46). – С. 32-38. – DOI 10.14529/secur220404. – EDN ZATSLM.

8. Yaparova, N. M. Mathematical modelling and method for solving a parametric identification problem for self-test of measuring devices / N. M. Yaparova // Inverse Problems in Science and Engineering. – 2016. – Vol. 24, No. 1. – P. 77-91. – DOI 10.1080/17415977.2015.1017482. – EDN NCXSNG.

9. Russakovsky O., Deng J., Su H. et al. ImageNet large scale visual recognition challenge. Int. J. of Computer Vision, 2015, vol. 115, no. 3, pp. 211–252. DOI: 10.1007/s11263-015-0816-y.

10. Sutton R.S., Barto A.G. Reinforcement Learning: An Introduction. Cambridge, The MIT Press, 2014, 338 p. 5. Silver D., Huang A., Maddison C.J. et al. Mastering the game of Go with deep neural networks and tree search. Nature, 2016, vol. 529, no. 7587, pp. 484–489. DOI: 10.1038/nature16961.

11. Mingxing T., Quoc V.L. EfficientNet: Rethinking model scaling for convolutional neural networks. ArXiv, 2019, art. 1905.11946v5. URL: https://arxiv.org/pdf/1905.11946.pdf (дата обращения: 17.06.2022).

12. Abdolmaleki A., Springenberg J.T., Degrave J. et al. Relative entropy regularized policy iteration. ArXiv, 2018, art. 1812.02256. URL: https://arxiv.org/abs/1812.02256 (дата обращения: 18.06.2022).

13. Аверин П. И., Мельников Б. Ф. Вариант решения задачи прогнозирования признаков разрушения металлов с помощью нейронных сетей на основе данных вейвлет-анализа импульсов акустической эмиссии // Современные информационные технологии и ИТ-образование. 2011. №7.

14. Львов А. С. Повышение быстродействия в обучении нейронной сети многопараметрическому контролю процессов в металлургии на базе вычислителей низкой конфигурации / А. С. Львов, А. В. Полянский// Вестник Череповецкого государственного университета. 2010. №3.

15. Тухватулин И. Х. Оптимизация состава износостойких сплавов с помощью нейросетей / И. Х. Тухватулин, Л. Б. Долгополова, В. М. Колокольцев, Ю. П. Ланкин // Литейные процессы: Межрегиональный сб. науч. тр. Магнитогорск: МГТУ, 2000. - С. 40-43.

References

1. Kohavi, R. A study of cross-validation and bootstrap for accuracy estimation and model selection / R. Kohavi // Proceedings of the Fourteenth International Joint Conference on Artificial Intelligence. San Mateo, 1995. – Vol. 2, № 12. – P. 1137–1143.

2. Dropout: A Simple Way to Prevent Neural Networks from Overfitting / G. Hinton et al. // Journal of Machine Learning Research. – 2014. – Vol. 15. – P. 1929–1958.

3. Krizhevsky, A. Imagenet classification with deep convolutional neural networks/ A. Krizhevsky, I. Sutskever, G. Hinton // Proceedings of the 25th International Conference on Neural Information Processing Systems, NIPS. – 2012. – P. 1097–1105.

4. Diederik, P. Kihgma. Adam: A method for Stochastic Optimization, 2014 / Diederik P. Kihgma, Jimmy Ba // Proceedings of the 3rd International Conference on Learning Representations (ICLR).

5. Goodfellow I., Bengio Y., Courville A. Deep learning. Genet Program Evolvable Mach, 2018, vol. 19, pp. 305–307. DOI: 10.1007/s10710-017-9314-z.

6. Krizhevsky A., Sutskever I., Hinton G.E. ImageNet classification with deep convolutional neural networks. Communications of the ACM, 2017, vol. 60, no. 6, pp. 84–90. DOI: 10.1145/3065386.

7. Yaparov, D. D. Ocenka metoda vosstanovleniya vkhodnogo signala po zashumlennym dannym / D. D. Yaparov // Vestnik URFO. Bezopasnost' v informacionnoj sfere. – 2022. – № 4(46). – S. 32-38. – DOI 10.14529/secur220404. – EDN ZATSLM.

8. Yaparova, N. M. Mathematical modelling and method for solving a parametric identification problem for self-test of measuring devices / N. M. Yaparova // Inverse Problems in Science and Engineering. – 2016. – Vol. 24, No. 1. – P. 77-91. – DOI 10.1080/17415977.2015.1017482. – EDN NCXSNG.

9. Russakovsky O., Deng J., Su H. et al. ImageNet large scale visual recognition challenge. Int. J. of Computer Vision, 2015, vol. 115, no. 3, pp. 211–252. DOI: 10.1007/s11263-015-0816-y.

10. Sutton R.S., Barto A.G. Reinforcement Learning: An Introduction. Cambridge, The MIT Press, 2014, 338 p. 5. Silver D., Huang A., Maddison C.J. et al. Mastering the game of Go with deep neural networks and tree search. Nature, 2016, vol. 529, no. 7587, pp. 484–489. DOI: 10.1038/nature16961.

11. Mingxing T., Quoc V.L. EfficientNet: Rethinking model scaling for convolutional neural networks. ArXiv, 2019, art. 1905.11946v5. URL: https://arxiv.org/pdf/1905.11946.pdf (дата обращения: 17.06.2022).

12. Abdolmaleki A., Springenberg J.T., Degrave J. et al. Relative entropy regularized policy iteration. ArXiv, 2018, art. 1812.02256. URL: https://arxiv.org/abs/1812.02256 (дата обращения: 18.06.2022).

13. Averin P. I., Mel`nikov B. F. Variant resheniya zadachi prognozirovaniya priznakov razrusheniya metallov s pomoshh`yu nejronny`x setej na osnove danny`x vejvlet-analiza impul`sov akusticheskoj e`missii // Sovremenny`e informacionny`e texnologii i IT-obrazovanie. 2011. №7.

14. L`vov A. S. Povy`shenie by`strodejstviya v obuchenii nejronnoj seti mnogopara-metricheskomu kontrolyu processov v metallurgii na baze vy`chislitelej nizkoj konfiguracii / A. S. L`vov, A. V. Polyanskij// Vestnik Cherepoveczkogo gosudarstvennogo universiteta. 2010. №3.

15. Tuxvatulin I. X. Optimizaciya sostava iznosostojkix splavov s pomoshh`yu nejrosetej / I. X. Tuxvatulin, L. B. Dolgopolova, V. M. Kolokol`cev, Yu. P. Lankin // Li-tejny`e processy`: Mezhregional`ny`j sb. nauch. tr. Magnitogorsk: MGTU, 2000. - S. 40-43.

ЯПАРОВ Дмитрий Данилович, старший преподаватель кафедры математического обеспечения информационных технологий, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: iaparovdd@susu.ru

КАРМАНОВ Дмитрий Евгеньевич, инженер кафедры математического обеспечения информационных технологий, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: karmanovde@susu.ru

ЯПАРОВА Наталья Михайловна, доктор технических наук, доцент, заведующий кафедрой математического обеспечения информационных технологий ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: iaparovanm@susu.ru

YAPAROV Dmitriy Danilovich, Senior Lecturer of Mathematical Foundation of Information Technologies Department, Federal State Autonomous Educational Institution of Higher Education «South Ural State University (national research university)». 454080, Chelyabinsk, Lenin prospekt, 76. E-mail: iaparovdd@susu.ru

KARMANOV Dmitriy Danilovich, engineer of Mathematical Foundation of Information Technologies Department, Federal State Autonomous Educational Institution of Higher Education «South Ural State University (national research university)». Russia, 454080, Chelyabinsk, Lenin prospekt, 76. E-mail: karmanovde@susu.ru

YAPAROVA Natalia Mikchailovna, Dr.of Sci, Associate Professor, Head of Department of Mathematical Foundation of Information Technologies, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)". Russia, 454080, Chelyabinsk, Lenin prospekt, 76. E-mail: iaparovanm@susu.ru.

УДК 004.65 Вестник УрФО № 1(55) / 2025, с. 37–44

Сенцова А. Ю., Арсланова Г. И., Русинова Д. С. DOI: 10.14529/secur250104

МЕТОД МНОГОКРИТЕРИАЛЬНОГО ВЫБОРА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Данная статья посвящена решению актуальной проблемы выбора средств защиты информации (СрЗИ) в условиях роста количества угроз и расширения доступных на рынке решений. Авторами предлагается метод многокритериального выбора средств защиты информации, основанный на методике комплексной оценки структур. Метод включает девять основных этапов, от определения множества альтернатив до выбора наиболее рационального средства защиты. В рамках подхода учитываются как субъективные предпочтения экспертов и заказчиков, так и объективные технические характеристики средств защиты, включая их совместимость и функциональность. Приведен пример практического применения метода на примере выбора антивирусных программ, что подчеркивает универсальность предложенного подхода. Дальнейшее развитие метода направлено на его автоматизацию, что позволит снизить трудозатраты и повысить точность выбора оптимальных решений.

Ключевые слова: *информационная безопасность, многокритериальный, система защиты, поиск оптимального выбора, угрозы, информационные риски.*

Sentsova A. U., Arslanova G. I., Rusinova D. S.

THE METHOD OF MULTI-CRITERIA SELECTION OF INFORMATION SECURITY TOOLS

This article is devoted to solving the urgent problem of selecting information protection equipment (IPE) in the context of the growing number of threats and the expansion of solutions available on the market. The authors propose a method of multi-criteria selection of information protection means based on the technique of complex evaluation of structures. The method includes nine main stages, from the definition of a set of alternatives to the selection of the most rational means of protection. The approach takes into account both subjective preferences of experts and customers and objective technical characteristics of protection means, including their compatibility and functionality. An example of practical application of the method is given on the example of selecting anti-virus programmes, which emphasises the universality of the proposed approach. Further development of the method is aimed at its automation, which will reduce labour costs and increase the accuracy of selecting optimal solutions.

Keywords: *information security, multi-criteria, protection system, search for optimal choice, threats, information risks.*

Введение

На сегодняшний день проблема выбора средств защиты информации (СрЗИ) при планировании специалистом по информационной безопасности (ИБ) модульного состава СрЗИ становится все более актуальной и насущной в связи с расширением предложений и количества возможных альтернатив СрЗИ на рынке. Вместе с тем, при выборе СрЗИ специалист обязан не только руководствоваться нормативной правовой базой в области ИБ и функциональными возможностями тех или иных средств защиты, но и учитывать особенности объекта защиты, предпочтения владельца объекта защиты и возможность совместимости различных средств защиты между собой. Кроме того, для выбора средства защиты из множества альтернатив необходимо использовать метод, который учитывал бы не только субъективное мнение эксперта, но и объективные критерии выбора СрЗИ, которые представляют собой технические характеристики средства защиты, параметры совместимости, реализованные функции и независимые экспертные оценки, статистические данные по каждой из альтернатив.

Таким образом, для решения проблемы выбора СрЗИ специалисту необходим аналитический метод, позволяющий осуществить многокритериальный выбор между возможными альтернативами, предложенными современными поставщиками средств защиты информации, который учитывал бы все вышеперечисленные требования.

В статье предложен метод многокритериального выбора средств защиты информации, основанный на методике комплексной оценки структур описанный в [1]. Метод, предложенный в работе, учитывает критерии выбора различных альтернатив средств защиты, степень важности критерия для владельца объекта защиты, а также меру разумной точности измерения соответствующего критерия для объекта защиты.

Метод многокритериального выбора средств защиты информации базируется на методологии системного анализа и представляет собой пошаговый процесс, первым этапом которого является выбор возможных альтернатив СрЗИ, которые соответствуют классу автоматизированной информационной системы [2] или ее уровню защищенности [3] в соответствии с нормативными правовыми документами в области защиты информации [4], а последним этапом определение наиболее рациональной альтернативы для проектирования или модернизации системы защиты информации.

Для решения проблемы выбора средств защиты информации с помощью метода многокритериального выбора в работе выделено девять основных этапов:

1. определение множества альтернатив СрЗИ, исходя из оценки существующей системы защиты информации объекта защиты;

2. выявление специалистом множества (совокупности) частных критериев, характеризующих альтернативы СрЗИ;

3. построение матрицы критериев альтернатив СрЗИ;

4. составление матрицы бинарных предпочтений, которая содержит результаты попарных сравнений критериев средства защиты по важности;

5. вычисление весов частных критериев исходя из разброса векторных оценок, а также нахождение усредненных весов частных критериев, с учетом предпочтений заказчика, мнения эксперта и аналитических расчетов;

6. перевод векторных оценок СрЗИ в безразмерную величину с помощью значения кванты;

7. построение матрицы векторных оценок, отображающих в табличной форме критерии СрЗИ и направление их экстремума;

8. свертка векторных оценок в обобщенные скалярные оценки;

9. выбор наилучшей альтернативы на основе аналитических расчетов обобщенных скалярных оценок.

Для успешной модернизации существующей системы защиты информации необходимо тщательно изучить политику безопасности предприятия, определить и категорировать основные активы, выделить угрозы безопасности и уязвимости объекта защиты, построить модель угроз и посчитать риски нарушения информационной безопасности. После анализа уровня риска и основных уязвимостей компонентов инфраструктуры, принимается решение модернизировать существующую систему защиты информации и определяется множество альтернатив средств защиты информации, которые будут либо новым барьером на пути распространения угрозы, либо заменят другое средство защиты, уязвимость которого признана экспертами наиболее существенной.

Таблица 1

Матрица критериев альтернатив средств защиты информации

K_i / S_j	S_1	S_2	…	S_{n-1}	S_n	Направление экстремума
K_1	P_{11}	*P12*	…	$P_{1,n-1}$	P_{1n}	min/max
K_2	P_{21}	*P22*	…	$P_{2,n-1}$	P_{2n}	min/max
…	…	…	…	…	…	min/max
K_{m-1}	$P_{m-1,1}$	*Pm-1,2*	…	$P_{m-1,n-1}$	$P_{m-1,n}$	min/max
K_m	P_{m1}	*Pm2*	…	$P_{m,n-1}$	P_{mn}	min/max

Разработка многокритериального метода выбора средств защиты

Для выбора СрЗИ из множества альтернатив, специалист по защите информации должен выявить частные критерии, которые будут характеризовать каждую рассматриваемую в процессе выбора альтернативу. Выявление частных критериев выбора СрЗИ является творческой неформализуемой задачей, которая выполняется специалистом по защите информации на основе его знаний, опыта и характеристик, декларируемых производителем СрЗИ [5]. Для выявления таких критериев специалистом могут быть использованы любые инструменты для получения знаний об альтернативе: аналитические, статистические, имитационные и т.д. На основе полученных экспертом данных формируется множество частных критериев.

1. На начальном этапе для выбора СрЗИ специалисту в области ИБ нужно определить совокупность альтернатив, удовлетворяющих целевую функцию области исследования и совокупность частных критериев для оценки качественных и количественных характеристик СрЗИ.

2. На основе совокупности критериев $\{K_m\}$ и альтернатив СрЗИ $\{S_n\}$ строится матрица (Таблица 1) и выполняется количественная оценка (P_{ij}) СрЗИ по каждому критерию.

3. На следующем этапе составляется бинарная матрица предпочтений {Ki} (Таблица 2). Каждая ячейка в матрице – это результат попарного сравнения частных критериев по важности. 1 – если критерий строки важнее чем критерий столбца. 0,5 – если они равны. 0 – если важность критерия столбца выше, чем важность критерия строки.

Дополнительный столбец C_i – это общая оценка важности критерия, которая вычисляется по формуле 1:

$$C_i = \sum_{j=1}^{m} K_{ij}, \qquad (1)$$

Таблица 2

Бинарная матрица предпочтений

K_i	K_1	K_2	…	K_{m-1}	K_m	C_i
K_1	–	$K_1 \perp K_2$	…	$K_1 \perp K_{m-1}$	$K_1 \perp K_m$	$\sum_{j=1}^{m}(K_1 \perp K_j)$
K_2	$K_2 \perp K_1$	–	…	$K_2 \perp K_{m-1}$	$K_2 \perp K_m$	$\sum_{j=1}^{m}(K_2 \perp K_j)$
…	…	…	–	…	…	…
K_{m-1}	$K_{m-1} \perp K_1$	$K_{m-1} \perp K_2$	…	–	$K_{m-1} \perp K_m$	$\sum_{j=1}^{m}(K_{m-1} \perp K_j)$
K_m	$K_m \perp K_1$	$K_m \perp K_2$	…	$K_m \perp K_{m-1}$	–	$\sum_{j=1}^{m}(K_m \perp K_j)$

4. Следующим шагом эксперта станет вычисление весов частных критериев (Таблица 3), отражающих его предпочтение, исходя из разброса векторных оценок:

$$S_i^{\wedge} = \frac{1}{n} \times \sum_{j=1}^{n} S_{ij}, \quad (2)$$

$$\partial_{1i} = \frac{C_i}{\sum_{i=1}^{m} C_i}, \quad (3)$$

$$r_i = \frac{1}{n} \times \sum_{j=1}^{n} \frac{\left|S_{ij} - S_i^{\wedge}\right|}{S_i^{\wedge}}, \quad (4)$$

$$\partial_{2i} = \frac{r_i}{\sum_{i=1}^{m} r_i}. \quad (5)$$

5. Вычисляем усредненные веса частных критериев Ω_i, i=1, …, m.

$$\Omega_i = \alpha \times \partial_{1i} + \beta \times \partial_{2i}. \quad (6)$$

Коэффициенты α и β характеризуют степень доверия к весам, их сумма всегда равна 1.

6. На следующем этапе необходимо построить матрицу безразмерных оценок. Данная матрица включает в себя сведения из матрицы совокупности критериев и альтернатив и переменную ΔK. Переменная ΔK_i – это величина шага для частного критерия, при котором лицо, принимающее решение (ЛПР), реагирует на изменение значения критерия. Например, при подсчете скорости передачи информации в современном мире величина равная 1 Кб в большинстве случаев является неощутимой, незначительной для организации бизнес-процессов, а 10 Мбит напротив, может вызвать проблемы для реализации бизнес-процессов и может быть зафиксировано ЛПР. Также, эту величину можно считать мерой разумной точности измерения характеристики, то есть степенью приближения результатов расчетов по предлагаемому многокритериальному методу к некоторому действительному значению, которое необходимо учитывать при построении либо модернизации системы защиты информации на предприятии принимая во внимание предпочтения руководителя предприятия, построенную модель угроз (адаптированный базовый набор средств защиты) и требования нормативной правовой базы в области информационной безопасности.

В таблице 4 представлена матрица безразмерных оценок в общем виде. Столбец «Единицы измерения» заполняется в том случае, если у конкретного критерия можно выделить единицу измерения. Также, в случае такого критерия как «стоимость средства защиты информации», в данном столбце указывается, какое количество лицензий включает в себя данный критерий. Рекомендуется привести количество лицензий для конкретного средства защиты к единому значению.

7. Для приведения матрицы от безразмерной оценки к взвешенной оценке, необходимо значения СрЗИ по каждому критерию разделить на соответствующую величину кванты. Кванта рассчитывается по формуле 7:

$$P_{ij}^{new} = \frac{P_{ij}^{old}}{\Delta K_i}. \quad (7)$$

Таблица 3

Таблица весов частных критериев

K_i	$S_i^{\wedge}$	∂_{1i}	r_i	∂_{2i}
K_1	$\frac{1}{n} \times \sum_{j=1}^{n} S_{1j}$	$\frac{C_i}{\sum_{i=1}^{m} C_i}$	$\frac{1}{n} \times \sum_{j=1}^{n} \left\|S_{1j} - S_1^{\wedge}\right\|$	$\frac{r_1}{\sum_{i=1}^{m} r_i}$
K_2	$\frac{1}{n} \times \sum_{j=1}^{n} S_{2j}$	$\frac{C_i}{\sum_{i=1}^{m} C_i}$	$\frac{1}{n} \times \sum_{j=1}^{n} \left\|S_{2j} - S_2^{\wedge}\right\|$	$\frac{r_2}{\sum_{i=1}^{m} r_i}$
…	…	…	…	…
K_{m-1}	$\frac{1}{n} \times \sum_{j=1}^{n} S_{m-1j}$	$\frac{C_i}{\sum_{i=1}^{m} C_i}$	$\frac{1}{n} \times \sum_{j=1}^{n} \left\|S_{m-1j} - S_{m-1}^{\wedge}\right\|$	$\frac{r_{m-1}}{\sum_{i=1}^{m} r_i}$
K_m	$\frac{1}{n} \times \sum_{j=1}^{n} S_{mj}$	$\frac{C_i}{\sum_{i=1}^{m} C_i}$	$\frac{1}{n} \times \sum_{j=1}^{n} \left\|S_{mj} - S_m^{\wedge}\right\|$	$\frac{r_m}{\sum_{i=1}^{m} r_i}$

Таблица 4

Матрица безразмерных оценок

K_i	ΔK_i	Единицы измерения	S_1	S_2	…	$Sn\text{-}1$	Sn
K_1	ΔK_1		P_{11}	P_{12}	…	$P_{1n\text{-}1}$	P_{1n}
K_2	ΔK_2		P_{21}	P_{22}	…	$P_{2n\text{-}1}$	P_{2n}
…	…		…	…	…	…	…
$K_{m\text{-}1}$	$\Delta K_{m\text{-}1}$		$P_{m\text{-}11}$	$P_{m\text{-}12}$	…	$P_{m\text{-}1n\text{-}1}$	$P_{m\text{-}1n}$
K_m	ΔK_m		P_{m1}	P_{m2}	…	$P_{mn\text{-}1}$	P_{mn}

8. На данном этапе необходимо получить оценки мер эффективности (E) для каждой альтернативы по каждой характеристике при помощи обобщенных весов критериев как это показано на формуле 8:

$$E_{ij} = P_{ij} \times \Omega_i. \quad (8)$$

9. На заключительном этапе для нахождения наиболее рационального СрЗИ необходимо найти обобщенные скалярные оценки, путем нахождения разницы между суммарно взвешенными оценками со стороны минимизации и максимизации, по формуле 9:

$$Q_j = \sum_{e=max} S_{ej} - \sum_{e=min} S_{ej}. \quad (9)$$

Пример расчета выбора рационального варианта СрЗИ

Определимся с совокупностью альтернатив $\{S_i\}$ СрЗИ, рассматриваются антивирусные системы:

- Антивирус Dr.Web
- Kaspersky Antivirus
- ESET NOD32 антивирус

Критерии $\{K_i\}$ характерные для антивирусных систем:

- Стоимость [руб.]
- Необходимая минимальная частота процессора [ГГц]
- Необходимое минимальное количество ОЗУ [Мб]

Ниже в таблицах приведены результаты поэтапных вычислений.

Таблица 5

Матрица оценок эффективности

K_i	Ω_i	Единицы измерения	Направление экстремума (e)	S_1	S_2	…	$S_{n\text{-}1}$	S_n
K_1	Ω_1		min/max	E_{11}	E_{12}	…	$E_{1n\text{-}1}$	E_{1n}
K_2	Ω_2		min/max	E_{21}	E_{22}	…	$E_{2n\text{-}1}$	E_{2n}
…	…		min/max	…	…	…	…	…
$K_{m\text{-}1}$	$\Omega_{m\text{-}1}$		min/max	$E_{m\text{-}11}$	$E_{m\text{-}12}$	…	$E_{m\text{-}1n\text{-}1}$	$E_{m\text{-}1n}$
K_m	Ω_m		min/max	E_{m1}	E_{m2}	…	$E_{mn\text{-}1}$	E_{mn}

Таблица 6

Матрица критериев альтернатив средств защиты информации

K_i / S_j	S_1	S_2	S_3	Единицы измерения	Направление экстремума
K_1	1090	1320	990	Руб.	min
K_2	1,5	1	1,3	Ггц	min
K_3	512	2048	1024	Мб	min

Таблица 7

Бинарная матрица предпочтений

K_i	K_1	K_2	K_3	C_i
K_1		1	1	2
K_2	0		0,5	0,5
K_3	0	0,5		0,5

Таблица 8

Таблица весов частных критериев

K_i	S_i^	∂_{1i}	r_i	∂_{2i}
K_1	1133,3	0,6	0,109	0,151
K_2	1,26	0,16	0,14	0,193
K_3	1194.6	0,16	0,476	0,655

$$S_1^{\wedge} = \frac{1090+1320+990}{3} = 1133{,}3,$$

$$\partial_{11} = \frac{2}{2+0{,}5+0{,}5} \approx 0{,}6,$$

$$r_1 = \frac{1}{3} \times \left(\frac{|1090-1133{,}3|}{1133{,}3} + \frac{|1320-1133{,}3|}{1133{,}3} + \frac{|990-1133{,}3|}{1133{,}3} \right) = 0{,}109,$$

$$\partial_{21} = \frac{0{,}109}{0{,}109+0{,}140+0{,}476} = 0{,}151$$

Таблица 9

Матрица безразмерных оценок

K_i	ΔK_i	Единицы измерения	S_1	S_2	S_3
K_1	100	Руб	10,9	13,2	9,9
K_2	0,1	Ггц	15	10	13
K_3	100	Мб	5,12	20,48	10,24

$$P_{11}^{new} = \frac{1090}{100} = 10{,}9$$

Таблица 10

Матрица оценок мер эффективности

K_i	Ωi	Единицы измерения	Направление экстремума (e)	S_1	S_2	S_n
K_1	0,3755	Руб.	min	4,092	4,956	3,717
K_2	0,1765	Ггц	min	2,647	1,765	2,294
K_3	0,4075	Мб	min	2,086	8,345	4,172

$$\Omega_1 = 0{,}6 \times 0{,}5 + 0{,}151 \times 0{,}5 = 0{,}3755$$

$$E_{11} = 10{,}9 \times 0{,}3755 = 4{,}092$$

Согласно формуле 9 рассчитываем обобщенные скалярные оценки для каждой альтернативы. Результаты расчета для каждой из трех альтернатив:

- Q1 = – 8,825
- Q2 = – 15,066
- Q3 = – 10,183

Полученные в результате выполненных вычислений обобщенные скалярные оценки сравниваются между собой. Альтернатива Антивирус Dr.Web имеет наибольшую оценку и является наиболее рациональной среди данных альтернатив.

Значения обобщенных скалярных оценок могут принимать отрицательные значения, как в данном примере, в следствии того, что разные критерии имеют разные направления экстремума. Однако, опытным путем доказано, что количество оценок с разными направлениями экстремума не влияет на конечный результат нахождения наиболее рациональной альтернативы средства защиты информации.

В случае совпадений итоговый скалярных оценок нескольких альтернатив, рекомендуется внести дополнительный критерий, который помог бы сделать окончательный выбор в пользу той или иной альтернативы.

Процесс выбора наиболее рациональной альтернативы средства защиты из произвольного количества альтернатив по произвольному количеству критериев с помощью метода многокритериального выбора средств защиты информации, основанного на методике комплексной оценки структур, может быть реализован в виде программного кода, включающего в себя все перечисленные в статье этапы работы по методу.

Заключение

В статье предложен метод многокритериального выбора средств защиты информации, основанный на методике комплексной оценки структур, и представлен пример апробации данного метода с помощью выбора наиболее рациональной альтернативы из множества средств антивирусной защиты, представленных на рынке.

Метод позволяет осуществить рациональный выбор из произвольного количества альтернатив по произвольному количеству критериев. Отличительной особенностью метода является возможность учесть величину шага для частного критерия. Данный метод применим для количественных критериев, либо для критериев, которые были переведены из качественных в количественные.

Поскольку предложенный метод включает в себя большое количество этапов, а также сложные и трудоемкие расчеты, необходимо разработать программное средство, которое позволило бы автоматизировать все этапы метода многокритериального выбора средств защиты.

Дальнейшая работа будет направлена на автоматизацию метода и разработку программного средства, которое имело бы интуитивно понятный интерфейс для специалиста по информационной безопасности и позволило бы сократить время и трудозатраты на выбор рационального средства защиты из множества альтернатив с учетом их критериев.

Литература

1. Живицкая Е. Н. Системный анализ и проектирование [Электронный ресурс]. URL: http://victor-safronov.ru/systems-analysis/lectures/zhivickaya/21.html (дата обращения: 10.12.2024)

2. Руководящий документ Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. 30 марта 1992, 29 с.

3. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных.

4. Государственный реестр сертифицированных средств защиты инфор-мации [Электронный ресурс]. URL: https://reestr.fstec.ru/reg3 (дата обращения: 10.12.2024).

5. Яндыбаева Э.Э., Машкина И.В. Разработка модели планирования используемых средств защиты информации для информационной системы электронной торговой площадки / // Вестник УГАТУ. – 2015. – Том 19, № 1 (67). – С. 264–269

References

1. Zhivitskaya E. N. Sistemnyy analiz i proektirovanie [Elektronnyy resurs]. URL: http://victor-safronov.ru/systems-analysis/lectures/zhivickaya/21.html (data obrashcheniya: 10.12.2024)

2. Rukovodyashchiy dokument Avtomatizirovannye sistemy. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Klassifikatsiya avtomatizirovannykh sistem i trebovaniya po zashchite informatsii. 30 marta 1992, 29 s.

3. Postanovlenie Pravitel'stva RF ot 01.11.2012 N 1119 "Ob utverzhdenii trebovaniy k zashchite personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh.

4. Gosudarstvennyy reestr sertifitsirovannykh sredstv zashchity informatsii [Elektronnyy resurs]. URL: https://reestr.fstec.ru/reg3 (data obrashcheniya: 10.12.2024)

5. Yandybaeva E.E., Mashkina I.V. Razrabotka modeli planirovaniya ispol'zuemykh sredstv zashchity informatsii dlya informatsionnoy sistemy elektronnoy torgovoy ploshchadki / // Vestnik UGATU. – 2015. – Tom 19, № 1 (67). – S. 264–269

СЕНЦОВА Алина Юрьевна, кандидат технических наук, доцент кафедры вычислительной техники и защиты информации, федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский университет науки и технологий». 450076, Республика Башкортостан, г. Уфа, ул. Заки Валиди, д. 32. E-mail: sentsova.alina@yandex.ru

АРСЛАНОВА Гульназ Ильсуровна, студент кафедры вычислительной техники и защиты информации, федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский университет науки и технологий». 450076, Республика Башкортостан, г. Уфа, ул. Заки Валиди, д. 32. E-mail: arslanovagulnaz7@mail.ru

РУСИНОВА Дарья Сергеевна, студент кафедры вычислительной техники и защиты информации, федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский университет науки и технологий». 450076, Республика Башкортостан, г. Уфа, ул. Заки Валиди, д. 32. E-mail: rusinova_darya03@mail.ru

SENTSOVA Alina Yurievna, Candidate of Technical Sciences, Associate Professor of the Department of Computer Science and Information Security, Federal State Budgetary Educational Institution of Higher Education "Ufa University of Science and Technology". 450076, Republic of Bashkortostan, Ufa, Zaki Validi St., 32. E-mail: sentsova.alina@yandex.ru

ARSLANOVA Gulnaz Ilsurovna, student of the Department of Computer Science and Information Security, Federal State Budgetary Educational Institution of Higher Education "Ufa University of Science and Technology". 450076, Republic of Bashkortostan, Ufa, Zaki Validi St., 32. E-mail: arslanovagulnaz7@mail.ru

RUSINOVA Darya Sergeevna, student of the Department of Computer Engineering and Information Security, Federal State Budgetary Educational Institution of Higher Education "Ufa University of Science and Technology". 450076, Republic of Bashkortostan, Ufa, Zaki Validi St., 32. E-mail: rusinova_darya03@mail.ru

УДК 004.056 Вестник УрФО № 1(55) / 2025, с. 45–54

Костюченко К. Л., Вандышев И. С. DOI: 10.14529/secur250105

ПОЯВЛЕНИЕ НОВЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ПРИМЕНЕНИИ ДРОНОВ

В статье показано как инновационное транспортное средство – дрон – может стать угрозой безопасности информации. Представлена классификация современных беспилотных летательных аппаратов. Рассмотрены характеристики и сферы применения дронов. На основе реальных ситуаций и системного прогнозирования описываются угрозы, связанные с противозаконным использованием дронов, в т.ч. угрозы безопасности информации и угрозы объектам информатизации. Комплексный подход исследования заставляет по-новому взглянуть на проблемы обеспечения безопасности. Определяются меры защиты от преступного применения беспилотных летательных аппаратов. Представленный набор схем возможных негативных событий позволяет заранее предпринимать защитные меры.

Ключевые слова: *дрон, беспилотный летательный аппарат, угрозы безопасности информации, защита информации, объекты информатизации, антидроновые системы безопасности.*

Kostyuchenko K. L., Vandyshev I. S.

THE EMERGENCE OF NEW THREATS TO INFORMATION SECURITY WHEN USING DRONES

The article shows how an innovative vehicle – a drone – can become a threat to information security. The classification of modern unmanned aerial vehicles is presented. The characteristics and applications of drones are considered. Based on real-world situations and system forecasting, the threats asso-ciated with the illegal use of drones are described, including threats to information security and threats to informatization facilities. The comprehensive ap-proach of the research forces us to take a fresh look at security issues. Measures to protect against the criminal use of unmanned aerial vehicles are being de-fined. The presented set of schemes of possible negative events allows you to take protective measures in advance.

Keywords: *drone, unmanned aerial vehicle, threats to information security, information protection, objects of informatization, anti-drone security systems.*

Введение

Развитие науки и техники приводит к прогрессивным изменениям в жизни и деятельности человека. Однако в некоторых случаях добавляются и негативные побочные явления. Подобная ситуация сейчас складывается с дронами.

Поэтому целью данной статьи является показ того, как достаточно инновационное транспортное средство – дрон – может стать угрозой безопасности информации. Для этого будут рассмотрены классификация и сферы применения современных беспилотных летательных аппаратов, схемы создания дронами угроз безопасности информации и объектам ин-форматизации, а также меры нейтрализации этих угроз.

Классификация и применение дронов

Под термином «дрон» обычно понимается летательный аппарат без экипажа на борту – беспилотный летательный аппарат (БПЛА) или «беспилотник». Иногда этот термин трактуется шире. Дронами называют все аппараты, входящие в сообщество беспилотных мобильных средств, отличающихся разными средами функционирования (рис. 1) [1]. В разговорной речи термин «дрон», сужается до понятия «коптер» (или «квадрокоптер»), т.е. БПЛА вертолетного типа с несколькими роторами (чаще всего с четырьмя).

Первые дроны появились достаточно давно – в XIX веке – и стали активно использоваться военными. В период Мировых войн это были самолеты-мишени, летающие торпе-

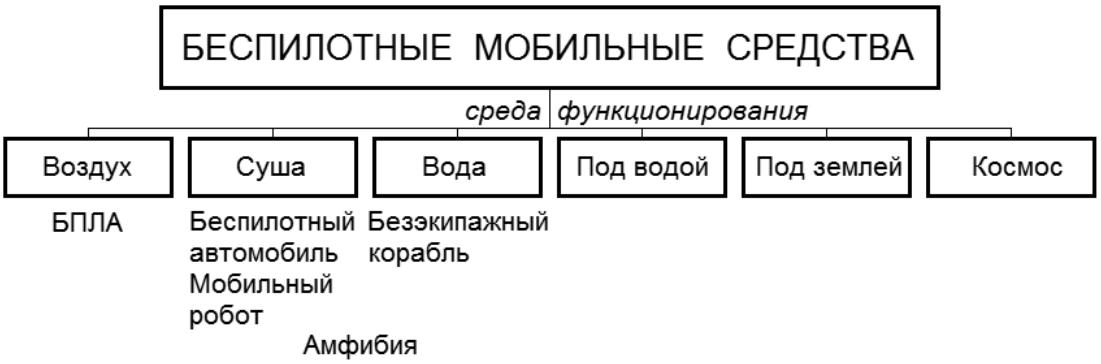

Рис. 1. Классификация беспилотных мобильных средств

Рис. 2. Классификация дронов

ды, реактивные беспилотные разведчики, крылатые ракеты и иные дистанционно-пилотируемые летательные аппараты (ДПЛА). В настоящее время БПЛА имеют различные типы конструкций с самыми разнообразными функциями и областями применения [2].

По основному критерию технической классификации – принципу полета – БПЛА делятся на следующие группы: аэростатического типа (дирижабли); с гибким крылом (мотопарапланы); с машущим крылом; с жестким крылом (самолеты); с вращающимся крылом (вертолетного типа), а различные гибриды (например, автожиры) (рис. 2).

Развитие техники, электроники, энергетики, информационных тех-нологий и программирования в начале XXI века определило тенденции в создании БПЛА:

- повышение энергоемкости тяговых аккумуляторов;
- применение новых конструкционных материалов;
- использование разнообразных конструкторских решений;
- уменьшение размеров (в целом и составных элементов);
- универсализация компоновки аппаратов;
- увеличение длительности полетов;
- повышение стабильности;
- постоянное появление новых функций.

Названные тенденции определили широту применения БПЛА (как гражданского, так и военного) (рис. 3). В гражданском применении это: мониторинг ЛЭП, теплосетей, трубопроводов, дорог, сооружений и иных объектов инфраструктуры; научные исследования (метеорология, эколо-гия, геология, археология); выполнение сторожевых функций; поисково-спасательные работы; фотосъемка и видеорепортажи; доставка грузов и еды (дроны-аэротакси, службы доставки); распыление химикатов (опыле-ние, вызов дождей); использование в системах связи; рекламные акции; свето-динамические шоу и др. В военном применении это: ведение разведки; целеуказание; объективный контроль (в реальном масштабе времени); гранато- и бомбометание; нанесение ударов летающими боеприпасами-«камикадзе»; доставка питания, боекомплекта и медикаментов; создание фиктивных целей; охрана объектов и патрулирование коммуникаций, радиоэлектронное подавление; ретрансляция данных [3]. К сожалению, существует и сфера неправомерного применения дронов (с различными целями: террористическими, криминальными и т.п.).

Большая доля применяемого арсенала дронов – мультироторные БПЛА – коптеры (в основном квадрокоптеры), оснащенные видеокамерой с передачей данных в реальном

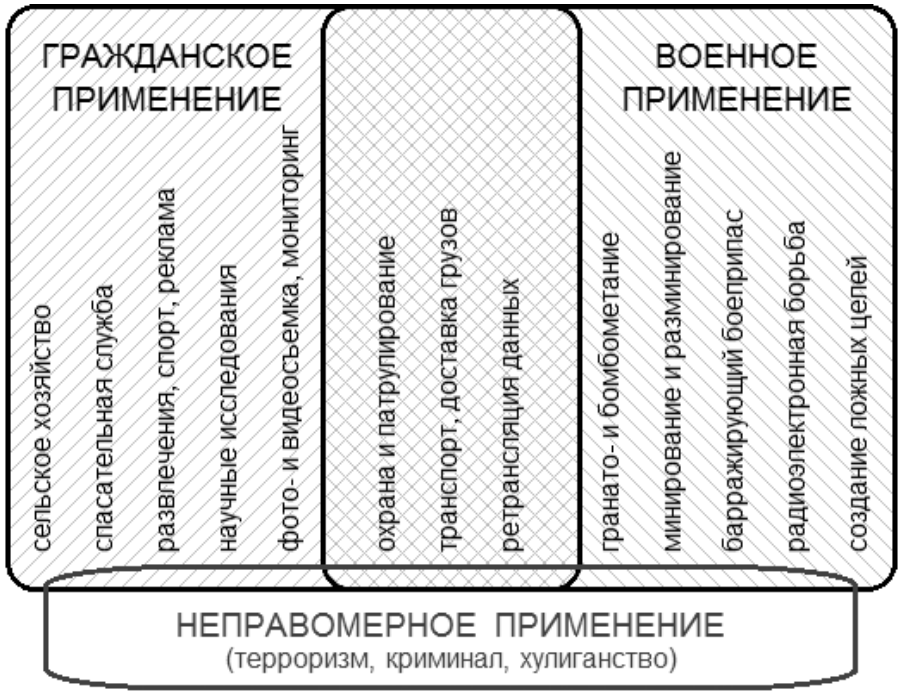

Рис. 3. Структура применения дронов

времени на пульт управления. Это так называемые «FPV-дроны» (First Person View – в переводе с английского – вид от первого лица). Основная особенность – использование оператором помимо обычного телевизионного канала очков виртуальной реальности (VR-очков) [4].

Благодаря своим оптимальным характеристикам, дроны вертолетного типа практически вытесняют остальные типы (может быть, за исключением тяжелых аппаратов самолетного типа).

Расширение сфер применения дронов, а, следовательно, и массовое производство привело к их удешевлению. Так, например, цена FPV-дронов составляет несколько десятков тысяч рублей, а в категории легких дронов – начинается с пары тысяч. Дешевизна и относительная простота конструкции и управления способствует вовлечению населения (молодежи) в новое увлечение (развлечение) – в создание и программирование дронов, а также в участие в конкурсах и различных соревнованиях.

С началом российской Специальной военной операции стало очевидно, что FPV-дроны стали одним из самых эффективных и дешевых вооружений. Дроны уверенно заняли нишу основного оружия на опера-тивно-тактическом уровне, потребовало небывалого расширения их производства. В этих условиях созданием и производством дронов приходится заниматься не только крупным фирмам и конструкторским бюро, но и многочисленным изобретателям-энтузиастам, изготавливающим аппараты практически «в полевых условиях». Разработки сразу проходят проверку в бою, после чего, согласно пожеланиями военных, подвергаются необходимым изменениям конструкции или корректировкам программного обеспечения, в целом подтверждая свои высокие качества.

Государство уделяет должное внимание дронам: в соответствии с потребностями появилась новая специальность – оператор FPV-дронов; в 2024 году начал свою работу национальный проект по развитию беспилотных авиационных систем; выделяются средства на обучение молодежи управлению дронами.

Необходимо отметить, что кроме прогресса в сфере БПЛА существует и значительный негатив, состоящий в противоправном использовании дронов. Резко увеличивающееся число произведенных аппаратов, значительная часть которых является неучтенными; постоянное совершенствование конструкции; расширение возможностей; отработанные тактики применения; низкая заметность; легкость управления; значительное число обученных операторов; отсутствие некоторых правовых норм не могут не привести к нарушению закона.

В криминологии известны похожие примеры, когда возникновение вооруженных конфликтов (и особенно их завершение) при наличии организованной преступности и пробелах в законодательстве влекут за собой неконтролируемое распространение оружия, боеприпасов и взрывных устройств. Вкупе с большим числом свободных обученных специалистов это привело к массе трагических ситуаций: заказные убийства, криминальные взрывы, ранения из-за неосторожного обращения с опасными предметами и т.п.

Для использования дронов в криминальных целях, некоторые из них даже не придется переделывать. Прежде всего, это касается «универсальных» конструкций, успешно используемых и в гражданской и военной сфере (рис. 3). Другие БПЛА могут дорабатываться, а определенная часть – специально выполняться под криминальные и террористические задачи. Такие задачи известны [3]: ведение постоянного наблюдения; доступ за охраняемые периметры; проникновение защищаемые помещения; точечное уничтожение отдельных важных персон; доставка (заброска) различных средств поражения; нанесение повреждений сооружениям, памятникам культуры, объектам инфраструктуры и подвижному составу; пермещение запрещенных средств; распыление опасных веществ; препятствование организации воздушного движения и т.д.

Угрозы безопасности информации и объектам информатизации

Что касается угроз безопасности информации, то применение дронов (чаще всего неправомерное) в составе технических каналов утечки информации только расширяет этот ряд.

Первые подобные эксперименты проводились полвека назад. Была разработана электромеханическая стрекоза со встроенным радиомикрофоном. Ввиду невысокой

энерговооруженности характеристики прообразов нынешних дронов были невысоки.

Сегодня проблемы увеличения емкости аккумуляторов во многом решены, и применение дронов может создавать широкий спектр информационных угроз. Некоторые такие угрозы очевидны. Это заброска «жучков», фото- и видеосъемка папарацци, наблюдение за частной жизнью и др. Другие только начинают оформляться либо уже скрыто существуют, но ввиду высокой степени закрытости (в сфере шпионажа, псевдошпионажа, промышленного шпионажа) просто нет никаких сведений.

Пока в статистических данных и в специальной литературе по защите информации и информационной безопасности, даже наиболее свежей, нет упоминания про применение дронов при слежке за человеком [5]. Но то, как дроны могут модифицировать технические каналы утечки информации и создать угрозы безопасности информации и объектам информатизации (ОИ) можно смоделировать. Примерный перечень возможных негативных ситуаций будет выглядеть следующим образом.

1. Фото- и видеосъемка в контролируемой зоне (КЗ) объекта информатизации (рис. 4). БПЛА, в первую очередь малые, ввиду слабой заметности могут достаточно просто проникать в КЗ. Более тяжелые и оснащенные сильной оптикой способны делать снимки на подлете к КЗ.

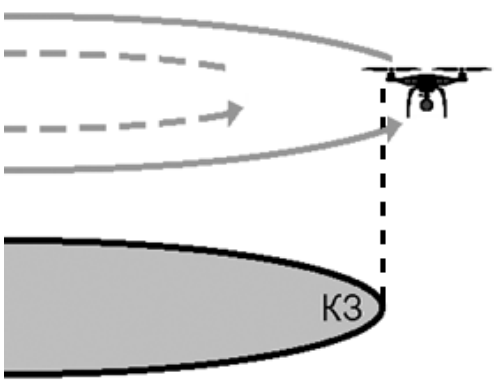

Рис. 4. Схема применения дрона для фото- и видеосъемки в контролируемой зоне (с заходом и без захода в нее)

2. Ретрансляция сигнала от устройства негласного съема информации (закладочного устройства, радиомикрофона), установленного на интересующем объекте (рис. 5). Ввиду того, что дрон может подлетать непосредственно к границе КЗ, радиопередающая часть закладки может быть выполнена менее мощной (и, соответственно, менее габаритной). Из-за этого поисковые мероприятия могут быть значительно затруднены, а для отлетевшего ретранслятора – вообще бесполезны.

Эта схема подходит и для сеансового приема информации, записанной ранее диктофоном (периодические подлеты дрона к границе КЗ).

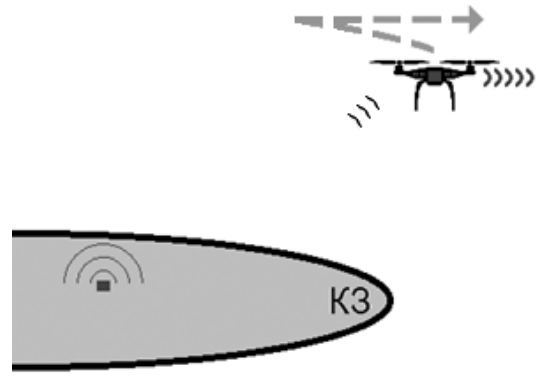

Рис. 5. Схема применения дрона для ретрансляции данных от устройств съема информации

3. Доставка различных устройств съема информации в зоны, где доступ человека затруднен, и в т.ч. не включенные ранее в КЗ (рис. 6).

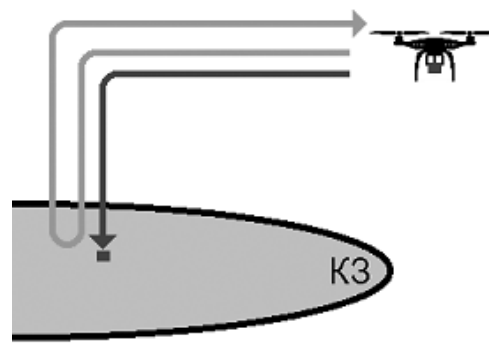

Рис. 6. Схема доставки различных устройств съема информации

4. Доставка в КЗ (или к границе КЗ) другого беспилотного мобильного средства (например, мобильного робота), способного самостоятельно перемещаться по поверхности до необходимой точки (удобной с точки зре-

ния съема или блокировки информации) (рис. 7).

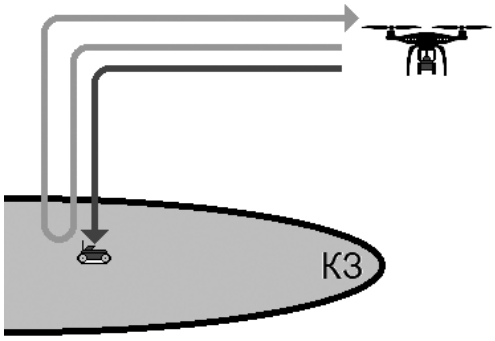

Рис. 7. Схема доставки беспилотного мобильного средства для съема или блокировки информации

5. Пролет дрона в КЗ с последующим превращением в устройство съема информации или источник электропитания (аналог дрона-камикадзе) (рис. 8).

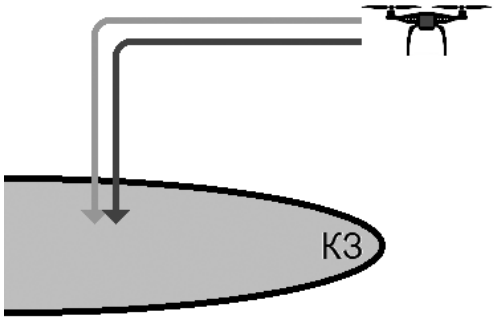

Рис. 8. Схема пролета дрона в КЗ с последующим превращением в устройство съема информации или источник электропитания

6. Пролет в КЗ с целью изъятия (кражи) носителей информации (документов, образцов и отходов производства) (рис. 9).

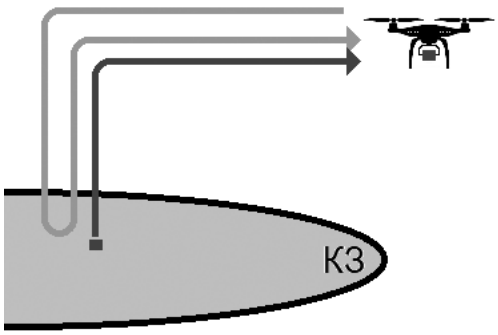

Рис. 9. Схема изъятия дроном носителей информации

7. Подавление сетей связи и цифровых каналов передачи данных (блокираторы, глушилки), как с заходом в КЗ, так и без этого (рис. 10).

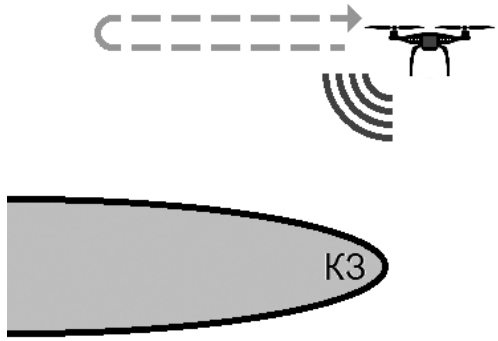

Рис. 10. Схема подавления дроном сетей связи и цифровых каналов пере-дачи данных

8. Различные варианты использования группы (роя) дронов, как в техническом, так и в тактическом плане, например, для отвлечения или перегрузки систем защиты (рис. 11).

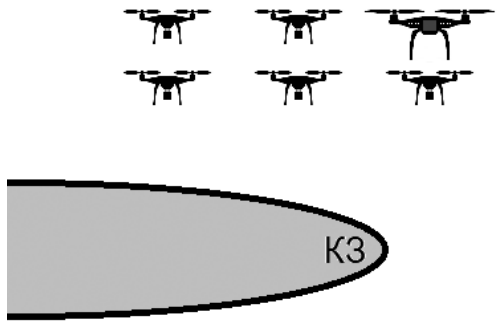

Рис. 11. Схема использования группы дронов

9. Столкновения дронов (в т.ч. случайные) объектами информатизации, ЛЭП, электрораспределительными устройствами (рис. 12). С повреждением устройств, линий, с отключением связи или электропитания.

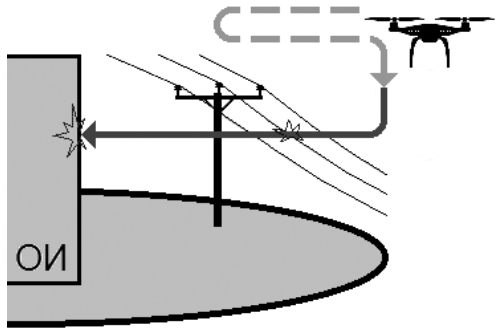

Рис. 12. Схема столкновений дронов (в т.ч. случайных) объектами информатизации, ЛЭП и т.п.

10. Сбрасывание различных предметов, листовок, фольги (или иных электропроводящих материалов над ЛЭП) (рис. 13). С нарушением работы различных устройств, с короткими замыканиями в ЛЭП и открытых распределительных электроустановках.

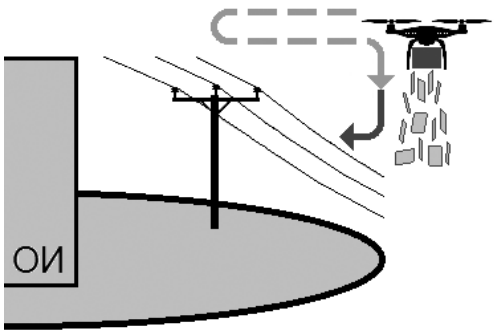

Рис. 13. Схема сбрасывания дронами фольги, листовок

11. Создание надписей на различных поверхностях (рис. 14). В зависимости от обстоятельств (как и сбрасывание листовок) может быть расценено правонарушением или преступлением (например, с антиконституционными призывами). По подобной схеме возможно и проецирование видеоинформации.

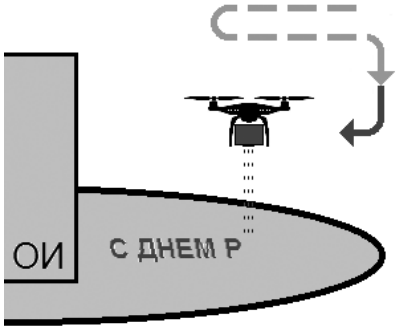

Рис. 14. Схема создания дронами надписей на различных поверхностях

12. Громкое звуковещание (с хулиганскими намерениями или для отвлечения сотрудников безопасности) (рис. 15).

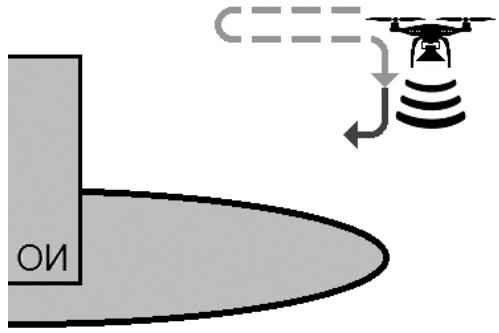

Рис. 15. Схема громкого звуковещания (например, для отвлечения)

Меры нейтрализации угроз

Обнаружить и нейтрализовать дроны достаточно сложно. Они постоянно совершенствуются, что делает перечисленные угрозы еще более актуальными. Поэтому необходимы надежные меры защиты от дронов. Их можно условно разделить на пассивные и активные (представлены на рис. 16). К пассивным мерам можно отнести организационно-правовые (требования законодательства и нормативных правовых актов; процедуры лицензирования; своевременное информирование) и инженерно-строительные (создание защищенных сооружений и специальных конструкций), а к активным мерам – реальное физическое противодействие – обнаружение; остановка; перехват управления; захват; ликвидация. Обнаружение может быть акустическим, оптическим, радарным и радиочастотным, а также их комбинацией. Противодействие может осуществляться при помощи радиоэлектронного подавления систем навигации и радиосвязи; воздействия СВЧ-излучения (для функционального поражения электроники дронов); перехвата (захвата) с использованием специальных дронов-перехватчиков, клейких и вязких аэрозолей, специально подготовленных птиц. В крайних случаях это может быть поражение при помощи огнестрельного оружия (прежде всего – дробового), лазерных систем, горючих химических смесей и т.п. [3, 6-8].

Указанный спектр мер противодействия в основном используется в военных условиях. Для гражданской сферы он сужается до разработки антидроновых систем с модуля-

ми направленной генерации помех. Характерным примером является постоянно совершенствующийся программно-аппаратный комплекс Kaspersky Antidrone, основанный на искусст-венном интеллекте и нейронных сетях, а также ему подобные системы [9].

Заключение

1. Дроны, несмотря на инновационное их применение в различных сферах, в других – могут становиться не только серьезными террористическими и криминальными угрозами, а и угрозами безопасности информации и объектам информатизации.

2. Несмотря на единичные зарегистрированные случаи противоправного использования дронов, уровень риска реализации таких угроз будет возрастать в связи с постоянным развитием науки и технологий, а также с происходящими социальными процессами (вооруженные конфликты, массовое хобби – конструирование и управление дронами и др.). При этом количественные показатели уровень риска можно рассчитать по появляющимся новым методикам [10].

3. Противоправное применение дронов во многом требует переосмысления некоторых базовых понятий информационной безопасности (контролируемая зона, физическая защита информации и др.).

4. Объекты информатизации и инфраструктуры в настоящее время требуют мер защиты от опасного использования дронов, которые заключаются в появлении новых специальных инженерно-строительных и конструкторских решений, а также в разработке программно-технических антидроновых систем.

5. Важным фактором, сдерживающим от неправомерного применения дронов, должно стать своевременное принятие необходимых норма-тивных правовых актов в сфере регламентации оборота беспилотных мобильных средств с последующим созданием эффективных механизмов их реализации.

6. Всё вышеописанное относительно дронов в определенной мере справедливо и для всей группы беспилотных мобильных средств. Поэтому можно заранее подготовить необходимые средства и планы противодействия возможным угрозам.

Рис. 16. Классификация средств противодействия противоправному применению дронов

Литература

1. Беспилотная авиация: терминология, классификация, современное состояние / В.С. Фетисов, Л.М. Неугодникова, В.В. Адамовский, Р.А. Красноперов; Под ред. В.С. Фетисова. – Уфа: ФОТОН, 2014. – 217 с.

2. Костюченко К. Л., Фараносов Д. А. Беспилотные мобильные средства: инновации и угрозы // Инновационный транспорт. 2024. №1 (50). С. 36-41.

3. Макаренко С.И., Тимошенко А.В., Васильченко А.С. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 1. Беспилотный летательный аппарат как объект обнаружения и поражения // Системы управления, связи и безопасности. 2020. № 1. С. 109-146.

4. Меринов К. FPV-дроны: технология, тактическое применение и будущее // Деловая газета «Взгляд». 15 сентября 2023 г. [Электронный ресурс]. URL: https://vz.ru/information/2023/9/15/1230301.html (дата обращения: 25.10.2023).

5. Новиков В.К., Краснов М.Г., Рекунков И.С. Средства, технологии, системы и технические каналы утечки информации для осуществления киберслежки за человеком и его деятельностью. – М.: Горячая линия – Телеком, 2023. – 160 с.

6. Макаренко С. И., Тимошенко А. В. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 2. Огневое поражение и физический перехват // Системы управления, связи и безо-пасности. 2020. № 1. С. 147-197.

7. Макаренко С. И. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 3. Радиоэлектронное подавление систем навигации и радиосвязи // Системы управления, связи и безопасности. 2020. № 2. С. 101-175.

8. Макаренко С. И. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 4. Функциональное поражение сверхвысокочастотным и лазерным излучениями // Системы управления, связи и безопасности. 2020. № 3. С. 122-157.

9. Kaspersky Antidrone – экосистема мониторинга и защиты от дронов // Лаборатория Касперского [Электронный ресурс]. URL: https:// antidrone.kaspersky.com/ru/ (дата обращения: 30.01.2025).

10. Повышев А. А., Соколов А. Н., Мищенко Е. Ю. Универсальная классификация угроз безопасности информации и её применение для разработки модели угроз и оценки рисков // Вестник УрФО. Безопасность в информационной сфере. 2023. № 3(49) С. 68–80.

References

1. Bespilotnaya aviaciya: terminologiya, klassifikaciya, sovremennoe sos-toya-nie / V.S. Fetisov, L.M. Neugodnikova, V.V. Adamovskij, R.A. Krasnope-rov; Pod red. V.S. Fetisova. – Ufa: FOTON, 2014. – 217 s.

2. Kostyuchenko K. L., Faranosov D. A. Bespilotnye mobil'nye sredstva: innovacii i ugrozy // Innovacionnyj transport 2024. № 1 (50). S. 36-41.

3. Makarenko S.I., Timoshenko A.V., Vasil'chenko A.S. Analiz sredstv i sposobov protivodejstviya bespilotnym letatel'nym apparatam. CHast' 1. Bes-pilotnyj letatel'nyj apparat kak obekt obnaruzheniya i porazheniya // Sistemy upravleniya, svyazi i bezopasnosti. 2020. № 1. S. 109-146.

4. Merinov K. FPV-drony: tekhnologiya, takticheskoe primenenie i bu-dushchee // Delovaya gazeta «Vzglyad». 15 sentyabrya 2023 g. [Elektronnyj resurs]. URL: https://vz.ru/information/2023/9/15/1230301.html (дата обращения: 25.10.2023).

5. Novikov V.K., Krasnov M.G., Rekunkov I.S. Sredstva, tekhnologii, sistemy i tekhnicheskie kanaly utechki informacii dlya osushchestvleniya kiber-slezhki za chelovekom i ego deyatel'nost'yu. – M.: Goryachaya liniya – Tele-kom, 2023. – 160 s.

6. Makarenko S. I., Timoshenko A. V. Analiz sredstv i sposobov protivodejstviya bespilotnym letatel'nym apparatam. CHast' 2. Ognevoe porazhenie i fizicheskij perekhvat // Sistemy upravleniya, svyazi i bezopas-nosti. 2020. № 1. S. 147-197.

7. Makarenko S. I. Analiz sredstv i sposobov protivodejstviya bes-pilotnym letatel'nym apparatam. CHast' 3. Radioelektronnoe podavlenie sistem navigacii i radiosvyazi // Sistemy upravleniya, svyazi i bezopasno-sti. 2020. № 2. S. 101-175.

8. Makarenko S. I. Analiz sredstv i sposobov protivodejstviya bes-pilotnym letatel'nym apparatam. CHast' 4. Funkcional'noe porazhenie sverhvy-sokochastotnym i lazernym izlucheniyami // Sistemy upravleniya, svyazi i bezopasnosti. 2020. № 3. S. 122-157.

9. Kaspersky Antidrone – ekosistema monitoringa i zashchity ot dronov // Laboratoriya Kasperskogo [Elektronnyj resurs]. URL: https:// anti-drone.kaspersky.com/ru/ (дата обращения: 25.10.2023).

10. Povyshev A. A., Sokolov A. N., Mishchenko E. YU. Universal'naya klassifi-kaciya ugroz bezopasnosti informacii i eyo primenenie dlya razrabotki mo-deli ugroz i ocenki riskov // Vestnik UrFO. Bezopasnost' v informaci-onnoj sfere. 2023. № 3(49) S. 68–80.

КОСТЮЧЕНКО Константин Леонидович, кандидат технических наук, доцент кафедры «Информационные технологии и защита информа-ции» федерального государственного бюджетного образовательного учреждения высшего образования «Уральский государственный университет путей сообщения». 620034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: KKostyuchenko@usurt.ru.

ВАНДЫШЕВ Иван Сергеевич, аспирант кафедры «Информационные технологии и защита информации» федерального государственного бюджетного образовательного учреждения высшего образования «Уральский государственный университет путей сообщения». 620034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: vandyschev.iwan@yandex.ru

KOSTYUCHENKO Konstantin Leonidovich, Candidate of Technical Sciences, Associate Professor of the Department of Information Technology and Information Protection of the Federal State Budgetary Educational Institution of Higher Education «Ural State University of Railway Transport». 620034, Yekaterinburg, Kolmogorova st., 66. E-mail: KKostyuchenko@usurt.ru.

VANDYSHEV Ivan Sergeevich, postgraduate student of the Department of Information Technology and Information Protection of the Federal State Budgetary Educational Institution of Higher Education «Ural State University of Railway Transport». 620034, Yekaterinburg, Kolmogorova st., 66. E-mail: vandyschev.iwan@yandex.ru.

УДК 004.056.5 Вестник УрФО № 1(55) / 2025, с. 55–61

Цуканов А. С., Соколов А. Н. DOI: 10.14529/secur250106

ОЦЕНКА ПОЛНОТЫ ПРИМЕНЯЕМЫХ МЕТОДОВ ПРИ ВНЕШНЕМ ТЕСТИРОВАНИИ НА ПРОНИКНОВЕНИЕ С УЧЕТОМ ВОЗМОЖНОСТЕЙ НАРУШИТЕЛЯ

Рассмотрены проблемы полноты и качества применяемых методов при проведении работ по тестированию на проникновение. Показано, что основным фактором, определяющим перечень таких работ, является техническое задание, которое, как правило, предлагается Исполнителем и составляется из соображений снижения его трудозатрат. При этом Заказчику, как правило, трудно оценить полноту, и, как следствие, качество таких работ. В статье предложен новый инструмент для оценки полноты и качества применяемых методов проведения работ по тестированию на проникновение, сформулирована проблематика выбора методов тестирования на проникновение с учетом возможностей нарушителя. Представлена модель оценки полноты применяемых методов при внешнем тестировании на проникновение на основе многодольного графа. На приведенном примере продемонстрирована эффективность представленной модели для выявления работ, не учтенных Исполнителем в предложенном техническом задании на проведение работ.

Ключевые слова: *вектор атаки, информационная безопасность, тестирование на проникновение, кибербезопасность, нарушитель, многодольный граф.*

ASSESSMENT OF THE COMPLETENESS OF THE METHODS USED IN EXTERNAL PENETRATION TESTING

The problems of completeness and quality of the methods used in conducting penetration testing are considered. It is shown that the main factor determining the list of such works is the terms of reference, which, as a rule, is proposed by the Contractor and is compiled from proposals to reduce his labor costs. At the same time, it is usually difficult for the Customer to assess the completeness and, as a result, the quality of such work. The article proposes a new tool for assessing the completeness and quality of the methods used for conducting penetration testing, and formulates the problems of choosing methods for penetration testing, taking into account the capabilities of the intruder. A model for assessing the completeness of the methods used in external penetration testing based on a multipole graph is presented. The given example demonstrates the effectiveness of the presented model for identifying works that were not taken into account by the Contractor in the proposed terms of reference for the work.

Keywords: *attack vector, information security, penetration testing, cyberse-curity, intruder, multipole graph.*

Введение. Важной частью работ в обеспечении кибербезопасности явля-ется моделирование атак реальных злоумышленников. Организации, которые проводят для своих заказчиков работы по внешнему тестированию на проникновение (далее – Исполнители) зачастую проводят работы исключительно по техническому заданию, при этом используя не все возможные методы проведения тестирования на проникновение и оценивая не все слабые места инфраструктуры заказчиков [1].

Работы по тестированию на проникновение проходят на договорной основе и в качестве перечня проверок выступает техническое задание на проведение работ. Как правило, технические задания согласует Заказчик работ, но предлагает его Исполнитель работ. Исполнители зачастую разрабатывают свои технические задания на проведение тестирования на проникновение из расчета наименьших трудозатрат. С таким подходом очень сложно понять, действительно ли были проверены все ресурсы заказчика или Исполнитель нашел только один успешный вектор атаки [2].

Необходимо отметить важность дополнительных проверок инфраструктур Заказчика после внедрения им средств защиты информации, основываясь на рекомендациях Исполнителя. Зачастую возникают ситуации, когда Исполнители проверяют только те вектора атак, которые ранее были успешны, не взяв в расчет то, что внедренные средства информационной безопасности также требуют проверки на возможность взлома [3].

В момент окончания работ возможно два результата: инфраструктура скомпрометирована или нет. В случае, если результат работ: инфраструктура не взломана, необходимо ответить на два вопроса:

1. Охватывает ли техническое задание, используемое Исполнителем, все задействованные ИТ-технологии заказчика?

2. Использованы ли все возможные тактики и техники реализации атак?

Рассмотрим пример проведения тестирования на проникновение с применением оценки применяемых тактик и техник нарушителя.

Пример. Злоумышленник взламывает личные кабинеты пользователей интернет-магазина и получает данные привязанных банковских карт.

Вектором атаки в этом случае является следующая последовательность действий:

1. Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений [4].

2. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке [4].

Для оценки качества выполненных работ по тестированию на проникно-вение введем следующие определения: *полнота работ по тестированию на проникновение* (далее – *полнота*) – это состояние работ, при котором реализуемые проверки затрагивают все используемые технологии и средства обработки информации. В свою очередь, *полнота применяемых методов при внешнем тестировании на проникновение* (далее – *полнота применяемых методов*) – это состояние работ, при котором реализуемые проверки (с использованием и без использования специально программного обеспечения) затрагивают все используемые технологии и средства обработки информации.

Вполне вероятной может оказаться ситуация, при которой рассмотрены все возможные технические векторы атак, но не учтены возможные ошибки, связанные с человеческим фактором. Для исключения этих ошибок рассмотрим модель оценки полноты работ по внешнему тестированию на проникновение на основе многодольного графа с учетом тактик и техник возможных вредоносных воздействий потенциальных злоумышленников (нарушителя).

Рассматриваемая модель имеет следующие ограничения:

1. Анализируются действия только внешнего нарушителя – злоумышленника, который не знает о внутреннем устройстве организации и действует со стороны сети «Интернет».

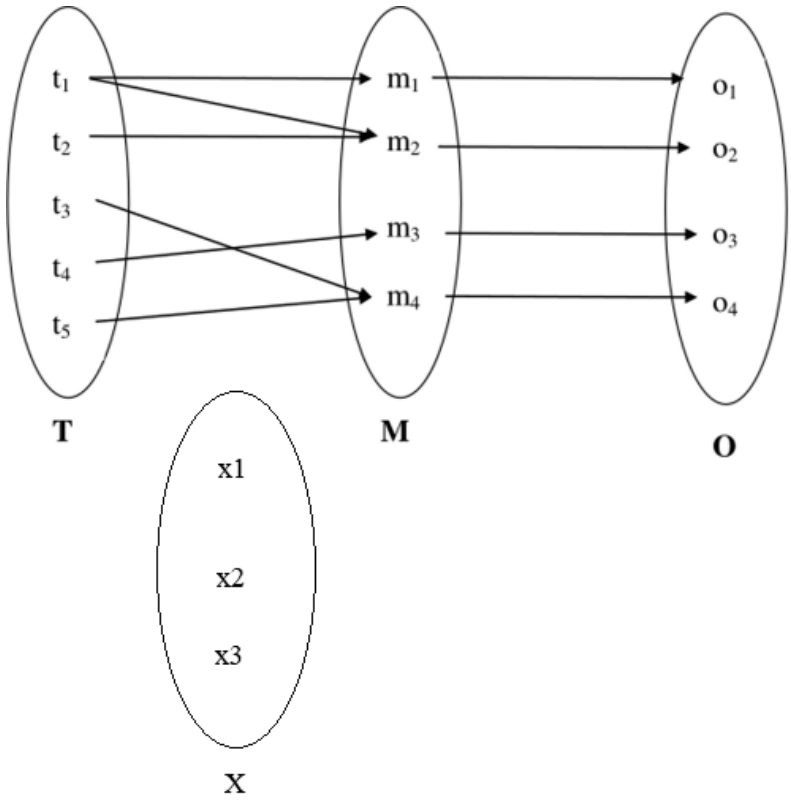

Рис. 1. Частный случай четырехдольного графа, описывающего полноту применяемых методов при внешнем тестировании на проникновение

2. Не рассматриваются технологии защиты информации, используемые организацией.

Модель реализуется на основе четырехдольного графа [5] (рис. 1), в котором:

1. Первая доля (M) — это используемые ИТ-технологии, которые проверяются в ходе работ (например, веб-сайты, JWT-токены и т.д.) [6, 7].

2. Вторая доля (T) — это всевозможные методы проверки при тестировании на проникновение, например, атака перебором (bruteforce) пароля и т.д. [8].

3. Третья доля (O) — потенциал нарушителя, который реализует угрозы безопасности информации. В качестве примера рассмотрим нарушителя с низким потенциалом, который используют только бесплатные инструменты для атаки.

4. Четвертая доля (X) — тактики и техники, реализуемые без использование специального программного обеспечения, которые не могут быть перекрыты средствами защиты информации.

5. Ребра, которые соединяют доли — это взаимосвязи между компонен-тами M, T, O и X. Например, если в первой доле (M) есть веб-сайт с личным кабинетом, то ему, как минимум, из второй доли (T) будет соответствовать атака по перебору паролей, а в третьей доле (O) будет указан низкий потенциал нарушителя, а в четвертой доле будет поиск логинов и паролей пользователей в публичных утечках.

Заметим, что не все вершины из доли T могут быть связаны с вершинами доли M по причине не совместимости используемой технологии и метода проверки. Примером такого исключения может быть метод проверки bruteforce пароля к используемой технологии «реализация https соединения».

Таким образом, для того, чтобы оценить полноту применяемых методов при внешнем тестировании на проникновение со стороны исполнителя, необ-ходимо выяснить: все ли вершины из первой доли (M), которые соединены с вершинами из третьей доли (O), были связаны с вершинами из второй (T) и четвертой (X) долей.

Рассмотрим представленный выше пример для оценки полноты приме-няемых методов технического задания Исполнителя, в котором отсутствует сценарий компрометации

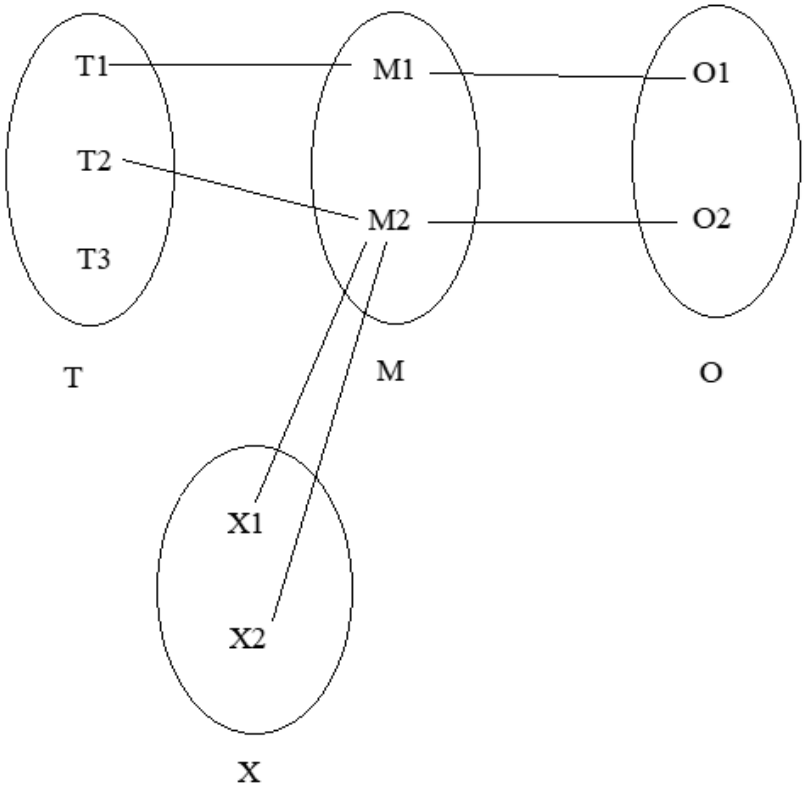

Рис. 2. Четырёхдольный граф, описывающий пример для оценки полноты применяемых методов при внешнем тестировании на проникновение на основе модели нарушителя

инфраструктуры без использования специального программного обеспечения: поиск информации в открытых источниках с использованием графа (рис. 2):

1. Определим доли графа:

1.1. M – форма для ввода данных (M1), форма для ввода логина и пароля (M2).

1.2. T – sql-инъекции (T1), bruteforce (T2), модификация сетевого тра-фика (T3).

1.3. O – потенциал нарушителя низкий (может выполнить атаки на формы M1 и M2, используя проверки/атаки T1 и T2).

1.4. X – поиск информации в открытых источниках (X1), поиск инфор-мации в darknet (X2).

2. Технологии M1 соответствует проверка T1, технологии M2 соответствует проверка T2 и техники X1 и X2.

3. Сверим ребра M1 – T1, M2 – T2, M2 – X1 и M2 – X2 с техническим заданием на проведение работ и видим, что поиск информации в открытых источниках и сети darknet не произведен.

4. Делаем вывод, что работы по тестированию на проникновение выполнены не в полном объеме, проверяемый ресурс находится под угрозой. Требуется актуализация технического задания на проведение работ.

Но, представленный таким образом граф, описывающий полноту применяемых методов при внешнем тестировании на проникновение на основе технического задания на проведение работ, не позволяет оценить их избыточность с целью экономии ресурсов.

С целью повышения качества работы модели по оценке полноты применяемых методов при внешнем тестировании на проникновение необходимо:

1. Рассмотреть варианты расширения модели за счет увеличения количество долей в исследуемом графе, например, путем учета средств защиты информации, добавления вероятностей атак для злоумышленника и т.д.

2. Использовать алгоритмы обхода графов [10] для минимизации количества проверок, которые необходимо пройти, для охвата всех используемых технологий обработки информации.

Таким образом, в работе сформулировано определение применяемых методов при внешнем тестировании на проникновение и рассмотрена ее модель на основе многодольного графа. В представленном примере на основе анализа модели продемонстрирован способ выявления работ, не учитываемых Исполнителем в техническом задании на проведение работ. Приведены варианты развития модели, позволяющие повысить качество оценки полноты работ по тестированию на проникновение.

Литература

1. Иванов, А. В. Вопросы оценки эффективности аудита информационной безопасности / А. В. Иванов, И. А. Огнев, В. В. Селифанов // Вестник УрФО. Безопасность в информационной сфере. – 2024. – № 4(54). – С. 37-48. – DOI 10.14529/secur240405. – EDN MGIOHA.

2. Макарова, О. С. Разработка методики прогнозирования динамики изменения вектора компьютерной атаки с точки зрения нарушителя: специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность»: диссертация на соискание ученой степени кандидата технических наук / Макарова Ольга Сергеевна, 2021. – 218 с. – EDN AEEOAG.

3. Сергеев, С. С. Методика построения графа атак для объектов критической информационной инфраструктуры / С. С. Сергеев, И. И. Баранкова // Вестник УрФО. Безопасность в информационной сфере. – 2022. – № 3(45). – С. 47-53. – DOI 10.14529/secur220305. – EDN SWZHQP.

4. Методика оценки угроз безопасности информации. Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 20.03.2025).

5. Алексеев В.Е, Захарова Д.В. ТЕОРИЯ ГРАФОВ: Учебное пособие. – Нижний Новгород: Нижегородский госуниверситет, 2017. –119 с.

6. Кинтонова А. Ж., Баенова Г. М., Урынбасарова А. Ж. Вопросы безопасности веб приложений // Colloquium-journal. 2020. №13 (65). Режим доступа: https://cyberleninka.ru/article/n/voprosy-bezopasnosti-veb-prilozheniy (дата обращения: 20.03.2025).

7. WebApplicationFirewall. Режим доступа: https://habr.com/ru/companies/otus/articles/733142/ (дата обращения: 20.03.2025).

8. OWASPtop 10. Режим доступа: https://owasp.org/www-project-top-ten/ (дата обращения: 20.03.2025).

9. Матрица атак MITRE ATT&CK. Режим доступа: https://mitre.ptsecurity.com/ru-RU (дата обращения: 20.03.2025).

10. Дольников, В. Л. Основные алгоритмы на графах: текст лекций / В. Л. Дольников, О. П. Якимова; Яросл. гос.ун-т им. П. Г. Демидова. – Ярославль: ЯрГУ, 2011. – 80 с.

References

11. Ivanov, A. V. Voprosy ocenki jeffektivnosti audita informacionnoj bezo-pasnosti / A. V. Ivanov, I. A. Ognev, V. V. Selifanov // Vest-nik UrFO. Bezopasnost' v informacionnoj sfere. – 2024. – № 4(54). – S. 37-48. – DOI 10.14529/secur240405. – EDN MGIOHA.

12. Makarova, O. S. Razrabotka metodiki prognozirovanija dinamiki izmenenija vektora komp'juternoj ataki s tochki zrenija narushitelja: special'nost' 05.13.19 "Metody i sistemy zashhity informacii, informacionnaja bezopasnost'": dissertacija na soiskanie uchenoj stepeni kandida-ta tehnicheskih nauk / Makarova Ol'ga Sergeevna, 2021. – 218 s. – EDN AEEOAG.

13. Sergeev, S. S. Metodika postroenija grafa atak dlja ob#ektov kri-ticheskoj informacionnoj infrastruktury / S. S. Sergeev, I. I. Barankova // Vestnik UrFO. Be-zopasnost' v informacionnoj sfere. – 2022. – № 3(45). – S. 47-53. – DOI 10.14529/secur220305. – EDN SWZHQP.

14. Metodika ocenki ugroz bezopasnosti informacii. Rezhim dostupa: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (data obrashhenija: 20.03.2025).

15. Alekseev V.E, Zaharova D.V. TEORIJa GRAFOV: Uchebnoe posobie. – Nizhnij Novgorod: Nizhegorodskij gosuniversitet, 2017. –119 s.

16. Kintonova A. Zh., Baenova G. M., Urynbasarova A. Zh. Voprosy bezopasnosti veb prilozhenij // Colloquium-journal. 2020. №13 (65). Rezhim dostupa: https://cyberleninka.ru/article/n/voprosy-bezopasnosti-veb-prilozheniy (data obrashhenija: 20.03.2025).

17. WebApplicationFirewall. Rezhim dostupa: https://habr.com/ru/companies/otus/articles/733142/ (data obrashhenija: 20.03.2025).

18. OWASPtop 10. Rezhim dostupa: https://owasp.org/www-project-top-ten/ (data obrashhenija: 20.03.2025).

19. Matrica atak MITRE ATT&CK. Rezhim dostupa: https://mitre.ptsecurity.com/ru-RU (data obrashhenija: 20.03.2025).

20. Dol'nikov, V. L. Osnovnye algoritmy na grafah: tekst lekcij / V. L. Dol'nikov, O. P. Jakimova; Jarosl. gos. un-t im. P. G. Demidova. – Jaroslavl': JarGU, 2011. – 80 s.

ЦУКАНОВ Александр Сергеевич, аспирант кафедры защиты информации ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: tsukanovas@susu.ru

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: sokolovan@susu.ru

TSUKANOV Aleksandr Sergeevich, post-graduate student of the Information Security, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)". 454080, Chelyabinsk, Lenina Avenue, 76. E-mail: tsukanovas@susu.ru

SOKOLOV Alexander Nikolayevich, Candidate of Technical Sciences, Associate Professor, Head of Department of Information Security, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)". 454080, Chelyabinsk, Lenina avenue, 76. E-mail: sokolovan@susu.ru.

УДК 004.056.53 Вестник УрФО № 1(55) / 2025, с. 62–69

**Кушнир Н. В., Яцкевич Е. С.,
Власенко А. В., Копцов С. В.**

DOI: 10.14529/secur250107

ПЕРЕДОВЫЕ ПОДХОДЫ К ОЦЕНКЕ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Растущая зависимость от цифровых технологий повысила важность обеспечения безопасности объектов критической информационной инфраструктуры (КИИ), которые жизненно важны для национальной безопасности, экономической стабильности и общественной безопасности.

В данной статье рассматриваются современные подходы к оценке безопасности объектов КИИ в России, с акцентом на методологии, основанные на оценке рисков, соблюдении требований законодательства и технологиях с применением технологий искусственного интеллекта.

На основе всестороннего анализа существующих методов оценки безопасности, тематических исследований из ключевых секторов, таких как энергетика, финансы и здравоохранение, а также оценки новых тенденций, таких как искусственный интеллект (ИИ) и машинное обучение, в этом исследовании определена методика оценки защищенности КИИ с применением современных подходов и технологий.

Результаты подчеркивают необходимость интеграции передовых технологий, повышения осведомленности о безопасности, ориентированной на человека, и обеспечения соответствия нормативным требованиям для противодействия возникающим киберугрозам.

Ключевые слова: *критическая информационная инфраструктура, искусственный интеллект, оценка защищённости, киберугроза, кибератака, методика оценки.*

Kushnir N. V., Yatskevich E. S., Vlasenko A. V., Koptsov S. V.

ADVANCED APPROACHES TO ASSESSING THE SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

The growing dependence on digital technologies has increased the importance of ensuring the security of critical information infrastructure facilities, which are vital for national security, economic stability, and public safety.

This article examines modern approaches to assessing the safety of CII facilities in Russia, with an emphasis on methodologies based on risk assessment, compliance with legal requirements and technology.

Based on a comprehensive analysis of existing security assessment methods, case studies from key sectors such as energy, finance and healthcare, as well as an assessment of new trends such as artificial intelligence (AI) and machine learning, this study defines a methodology for assessing the security of CII using modern approaches and technologies.

The results highlight the need to integrate cutting-edge technologies, raise awareness of human-centered security, and ensure regulatory compliance to counter emerging cyber threats.

Keywords: *critical information infrastructure, artificial intelligence, security assessment, cyber threat, cyber attack, assessment methodology.*

Введение

Критическая информационная инфраструктура (КИИ) представляет собой основу современного общества, охватывая системы и активы, необходимые для поддержания экономической стабильности, общественной и национальной безопасности. Эти инфраструктуры охватывают широкий спектр секторов, включая энергетику, финансы, здравоохранение, транспорт и государственные услуги. В России, растущая интеграция цифровых технологий в КИИ значительно повысила операционную эффективность, но также привела к появлению новых уязвимостей [1,2]. Киберугрозы, стихийные бедствия, инсайдерские риски и технические сбои создают серьезные проблемы для безопасности этих жизненно важных систем [3].

Растущая сложность и частота кибератак, нацеленных на объекты КИИ, подчеркивают настоятельную необходимость в надежных и адаптивных подходах к оценке безопасности. Традиционные методы, хотя и являются основополагающими, часто не учитывают динамичный и сложный характер современных угроз. Обеспечение устойчивости КИИ требует всестороннего понимания как существующих уязвимостей, так и возникающих рисков. Без эффективной оценки безопасности критически важные системы по-прежнему подвержены потенциальным сбоям [4,5].

Защита КИИ имеет первостепенное значение для обеспечения бесперебойного функционирования основных служб и сохранения общественного доверия.

Оценка защищенности объектов КИИ с помощью искусственного интеллекта

Искусственный интеллект (ИИ) все чаще используется для повышения эффективности оценки безопасности объектов критической информационной инфраструктуры (КИИ). Инструменты, основанные на ИИ, включая машинное обучение (ML) и нейронные сети, предлагают расширенные возможности для выявления уязвимостей, прогнозирования угроз и автоматизации реагирования. Эти системы анализируют огромные объемы данных для выявления аномалий, определения приоритетности рисков и предоставления

информации, пригодной для принятия мер по их устранению [6].

Например, системы обнаружения вторжений на базе искусственного интеллекта могут выявлять кибератаки и реагировать на них в режиме реального времени, в то время как инструменты поведенческой аналитики отслеживают активность пользователей для выявления внутренних угроз. Несмотря на преимущества, такие проблемы, как качество данных, техническая сложность и этические соображения, остаются. Будущие достижения, скорее всего, будут направлены на интеграцию ИИ с новыми технологиями, обеспечение понятности и противодействие враждебным атакам. Используя ИИ, организации могут применять упреждающий и адаптивный подход к защите объектов КИИ от возникающих угроз.

Уровни защищенности представляют собой гипотетические категории, которые могут обозначать различные аспекты или степени защиты системы.

Для анализа выделены следующие уровни защищенности:

Уровень 1: базовая защита, включающая стандартные меры безопасности, такие как антивирусное ПО и брандмауэры.

Уровень 2: улучшенная защита, добавляющая механизмы обнаружения вторжений и регулярные обновления безопасности.

Уровень 3: продвинутая защита, включающая шифрование данных, многофакторную аутентификацию и мониторинг безопасности в реальном времени.

Уровень 4: высокий уровень защиты с использованием машинного обучения для анализа угроз и автоматического реагирования на инциденты.

Уровень 5: максимальная защита, включающая все вышеперечисленные меры, а также проактивные стратегии, такие как симуляции атак и постоянное совершенствование системы безопасности [7,8].

Данные для анализа представлены в отчетах организаций, которые интегрировали ИИ в свои системы безопасности, такие как Ideco, Staffcop, Сбербанк и многие другие вендоры передовых информационных технологий. Зависимость защищенности представлена на рисунке 1.

Методика анализа защищенности системы с применением ИИ

Методология анализа безопасности объектов КИИ с использованием искусственного интеллекта (ИИ) предполагает структурированный подход, который объединяет качественные и количественные методы. В нем используются инструменты искусственного интеллекта, такие как машинное обучение, нейронные сети и предиктивная аналитика,

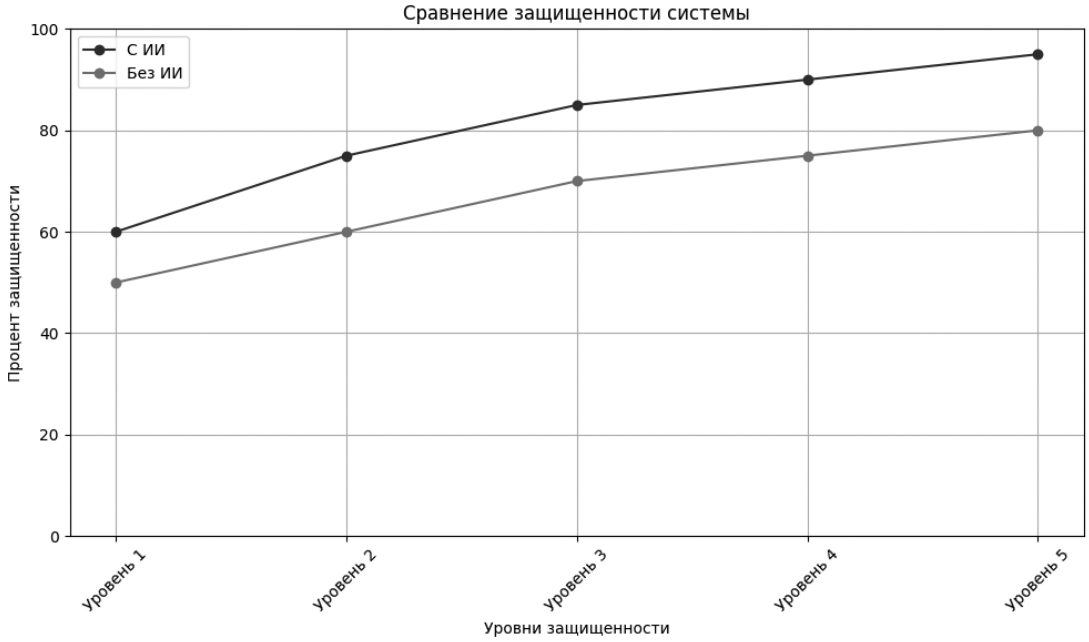

Рис. 1. Сравнения защищенности системы с применением ИИ

Таблица 1

Источники данных для анализа безопасности на основе искусственного интеллекта

Источник данных	Описание	Назначение в модели искусственного интеллекта
Журналы сетевого трафика	Журналы входящего / исходящего трафика	Обнаружение аномалий и потенциальных вторжений
Системные журналы	Журналы системных событий и ошибок	Выявление неправильных настроек или сбоев
Отчеты о сканировании уязвимостей	Результаты автоматического сканирования слабых мест	Определение приоритетности уязвимостей
Исторические данные об инцидентах	Записи прошлых кибератак и ответов	Обучение прогностическим моделям
Каналы анализа угроз	Обновления о возникающих угрозах в режиме реального времени	Усиление механизмов упреждающей защиты

для оценки уязвимостей, прогнозирования угроз и улучшения процесса принятия решений [9].

В исследовании используется гибридный подход, сочетающий в себе:

• Качественный анализ: интервью с экспертами по кибербезопасности и анализ документов для получения информации о современных методах обеспечения безопасности.

• Количественный анализ: использование алгоритмов, управляемых искусственным интеллектом, для обработки больших массивов данных для обнаружения угроз, оценки рисков и смягчения последствий.

Платформа, основанная на ИИ, фокусируется на трех основных компонентах:

1. Сбор и предварительная обработка данных.
2. Разработка и обучение модели ИИ.
3. Оценка эффективности и валидация.

Данные собираются из нескольких источников:

- Сетевые журналы: структура трафика, системные журналы и активность пользователей.
- Сканирование уязвимостей: результаты с помощью автоматизированных инструментов сканирования уязвимостей.
- Исторические данные об инцидентах: записи о прошлых кибератаках и взломах.
- Информация о внешних угрозах: данные из глобальных баз данных по кибербезопасности.

Аналитическая структура состоит из трех этапов:

Этап 1 – предварительная обработка данных.

Исходные данные очищаются и нормализуются для обеспечения совместимости с моделями искусственного интеллекта. Основные этапы предварительной обработки включают:

- Нормализация: масштабирование числовых характеристик до стандартного диапазона (например, 0-1).
- Извлечение признаков: определение релевантных признаков для анализа.
- Маркировка: присвоение меток историческим данным для контролируемого обучения (например, «нормальным» или «аномальным»).

Чтобы нормализовать функцию X до диапазона (0,1):

$$Xnormalized = \frac{X - Xmin}{Xmax - Xmin}, \qquad (1)$$

где

$Xmin$ и $Xmax$ – это минимальное и максимальные значения функции.

Этап 2 – разработка модели искусственного интеллекта.

Модели искусственного интеллекта обучены анализировать риски безопасности и уязвимости. Распространенные модели включают:

1. Контролируемое обучение: для обнаружения известных угроз (например, классификационных моделей, таких как случайный лес или машины опорных векторов).

Таблица 2

Модели искусственного интеллекта и их приложения

Тип модели	Алгоритм	Приложения
Контролируемое обучение	Случайный лес	Классифицирует сетевой трафик как нормальный / аномальный
Неконтролируемое обучение	DBSCAN	Обнаруживает отклонения в поведении системы
Обучение с подкреплением	Q-Learning	Оптимизация автоматического реагирования на инциденты
Нейронные сети	Сверточные нейронные сети (CNN)	Анализ сигнатур вредоносных программ на основе изображений

2. Обучение без учителя: для выявления неизвестных угроз (например, алгоритмов кластеризации, таких как k-средние значения).
3. Обучение с подкреплением: для оптимизации стратегий реагирования на инциденты.

Аномалии обнаруживаются на основе отклонений от среднего значения:

$$P(X) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(X-\mu)^2}{2\sigma^2}}, \quad (2)$$

где

$P(X)$ – вероятность наблюдения значения X.

μ – среднее значение набора данных.

σ^2 – дисперсия набора данных.

Если $P(X) <$ пороговое значение, наблюдение помечается как аномальное.

Этап 3 – оценка эффективности.

Производительность моделей искусственного интеллекта оценивается с помощью таких показателей, как точность, прецизионность, отзыв и оценка F1. Кроме того, для визуализации результатов используются матрицы путаницы.

Истинные положительные результаты (True Positives, TP): случаи, когда модель правильно предсказывает положительный класс.

Истинные негативы (True Negatives, TN): случаи, когда модель правильно предсказывает отрицательный класс.

Ложноположительные результаты (FP): случаи, когда модель неверно предсказывает положительный класс (ошибка I типа).

Ложные отрицательные результаты (FN): случаи, когда модель неверно предсказывает отрицательный класс (ошибка II типа).

Точность: доля правильно идентифицированных аномалий среди всех прогнозируемых аномалий.

$$\text{Точность} = \frac{TP}{TP+FP}. \quad (3)$$

Отзыв: доля правильно идентифицированных аномалий среди всех фактических аномалий.

$$\text{Отзыв} = \frac{TP}{TP+FN}. \quad (4)$$

С помощью этих показателей оценивается эффективность предлагаемой модели с применением искусственного интеллекта.

Эта методология обеспечивает систематический способ анализа безопасности объектов КИИ с использованием искусственного интеллекта. Используя передовые алгоритмы и постоянный мониторинг, организации могут достичь высокого уровня защиты от возникающих киберугроз [10].

Таблица 3

Матрица путаницы для оценки модели искусственного интеллекта

Фактический/прогнозируемый результат	Нормальный	Аномальный
Нормальный	Истинно отрицательный (TN)	Ложноположительный (FP)
Аномальный	Ложноотрицательный (FN)	Истинно положительный (TP)

Таблица 4

Ключевые этапы методологии

Шаг	Описание	Результат
Сбор данных	Сбор сетевых журналов, сканирований уязвимостей и т.д.	Полный набор данных для обучения ИИ
Предварительная обработка данных	Нормализация и маркировка данных	Очистка и структурирование данных для анализа
Разработка модели ИИ	Обучение моделей под наблюдением / без присмотра	Обученная модель для обнаружения угроз
Оценка производительности	Оценивайте, используя такие показатели, как точность и отзыв,	Валидированная модель с высокой точностью
Соблюдение этических норм	Устраняет проблемы конфиденциальности, предвзятости и объяснимости	Этически обоснованная и прозрачная модель
Развертывание и валидация	Тестируйте модель в реальных сценариях	Функциональный инструмент искусственного интеллекта для обеспечения безопасности КИИ

Заключение

Разработанная методология можем применяться для оценки защищенности объектов критической информационной инфраструктуры и является актуальной для применяемых технологий в 2025 году.

Интеграция технологий искусственного интеллекта является передовой для большинства организаций в России, поэтому технологическая база во многих случаях не требует дополнительных надстроек для интеграции разработанной методики, в связи с чем результат существующей разработки имеет высокий потенциал для внедрения.

Литература

1. Обласов А. А. Организация и технология защиты конфиденциальной информации в информационных системах: методическое пособие для студентов. — М.: Ridero, 2020. — 173 с.

2. Степаненко С. И. ГосСОПКА в области критической информационной инфраструктуры Российской Федерации / С. И. Степаненко // The World of Science Without Borders, 11 февраля 2022 года, 2022. – Р. 348-350. – EDN RQKGRV.

3. Колтунова Т. В. Правовые аспекты обеспечения информационной безопасности в критической информационной инфраструктуре / Т. В. Колтунова, Н. Л. Колтунов // Евразийский юридический журнал. – 2022. – № 3(166). – С. 413-416. – EDN GBXTYW.

4. Максимова Е. А. Проактивное Управление информационной безопасностью субъектов критической информационной инфраструктуры как сложных организационных систем с динамически изменяющейся структурой / Е. А. Максимова, М. В. Буйневич, А. В. Шестаков // Вестник Воронежского института МВД России. – 2023. – № 2. – С. 49-59. – EDN CWISSD.

5. Долженков С. С. Оптимизация системы менеджмента информационной безопасности объектов критической информационной инфраструктуры / С. С. Долженков // Студенческая наука для развития информационного общества: Материалы ХУ Всероссийской научно-технической конференции с приглашением зарубежных ученых, Ставрополь, 28 ноября 2023 года. – Ставрополь: Северо-Кавказский федеральный университет, 2024. – С. 124-130. – EDN EYGAVD.

6. Фисун В. В. О необходимости интеллектуализации процессов управления информационной безопасностью на объектах критической информационной инфраструктуры / В. В. Фисун // Информационная безопасность - актуальная проблема современности. Совершенствование образовательных технологий подготовки специалистов в области информационной безопасности. – 2018. – № 1(9). – С. 255-257. – EDN JEGHAR.

7. Иконников С. Е. Создание системы защиты и автоматизация информационной безопасности на объектах критической информационной инфраструктуры / С. Е. Иконников // Интеллектуальные транспортные системы: Материалы III Международной научно-практической конференции, Москва, 30 мая 2024 года. – Москва: Российский университет транспорта (МИИТ), 2024. – С. 575-578. – DOI 10.30932/9785002446094-2024-575-578. – EDN RVIGBA.

8. Методика обеспечения устойчивости функционирования критической информационной инфраструктуры в условиях информационных воздействий / С. М. Климов, С. В. Поликарпов, Б. С. Рыжов [и др.] // Вопросы кибербезопасности. – 2019. – № 6(34). – С. 37-48. – DOI 10.21681/2311-3456-2019-6-37-48. – EDN ANVHWE.

9. Смирнов Г. Е. Актуальные вопросы развития теории и практики аудита информационной безопасности объектов критической информационной инфраструктуры / Г. Е. Смирнов, С. И. Макаренко // Проблемы комплексной безопасности Каспийского макрорегиона: Сборник научных статей по материалам международной научно-практической конференции, Астрахань, 28–29 октября 2021 года / Под общей редакцией А.П. Романовой, Д.А. Черничкина. – Астрахань: Астраханский государственный университет, Издательский дом "Астраханский университет", 2021. – С. 148-157. – EDN MSQRDC.

10. Воеводин В. А. О проблеме оценивания устойчивости функционирования объектов критической информационной инфраструктуры для условий воздействия угроз информационной безопасности / В. А. Воеводин // Радиоэлектронные устройства и системы для инфокоммуникационных технологий" ("РЭУС-ИТ 2024"): Доклады Всероссийской конференции, посвященной Дню радио, Москва, 31 мая 2024 года. – Москва: Российское научно-техническое общество радиотехники, электроники и связи им. А.С. Попова, 2024. – С. 299-304. – EDN UPBBWH.

References

1. Oblasov A. A. Organizatsiya i tekhnologiya zashchity konfidentsial'noy informatsii v informatsionnykh sistemakh: metodicheskoe posobie dlya studentov . — M.: Ridero, 2020. — 173 s.

2. Stepanenko S. I. GosSOPKA v oblasti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii / S. I. Stepanenko // The World of Science Without Borders, 11 fevralya 2022 goda, 2022. – P. 348-350. – EDN RQKGRV.

3. Koltunova T. V. Pravovye aspekty obespecheniya informatsionnoy bezopasnosti v kriticheskoy informatsionnoy infrastrukture / T. V. Koltunova, N. L. Koltunov // Evraziyskiy yuridicheskiy zhurnal. – 2022. – № 3(166). – S. 413-416. – EDN GBXTYW.

4. Maksimova E. A. Proaktivnoe Upravlenie informatsionnoy bezopasnost'yu sub"ektov kriticheskoy informatsionnoy infrastruktury kak slozhnykh organizatsionnykh sistem s dinamicheski izmenyayushcheysya strukturoy / E. A. Maksimova, M. V. Buynevich, A. V. Shestakov // Vestnik Voronezhskogo instituta MVD Rossii. – 2023. – № 2. – S. 49-59. – EDN CWISSD.

5. Dolzhenkov S. S. Optimizatsiya sistemy menedzhmenta informatsionnoy bezopasnosti ob"ektov kriticheskoy informatsionnoy infrastruktury / S. S. Dolzhenkov // Studencheskaya nauka dlya razvitiya informatsionnogo obshchestva: Materialy KhU Vserossiyskoy nauchno-tekhnicheskoy konferentsii s priglasheniem zarubezhnykh uchenykh, Stavropol', 28 noyabrya 2023 goda. – Stavropol': Severo-Kavkazskiy federal'nyy universitet, 2024. – S. 124-130. – EDN EYGAVD.

6. Fisun V. V. O neobkhodimosti intellektualizatsii protsessov upravleniya informatsionnoy bezopasnost'yu na ob"ektakh kriticheskoy informatsionnoy infrastruktury / V. V. Fisun // Informatsionnaya bezopasnost' - aktual'naya problema sovremennosti. Sovershenstvovanie obrazovatel'nykh tekhnologiy podgotovki spetsialistov v oblasti informatsionnoy bezopasnosti. – 2018. – № 1(9). – S. 255-257. – EDN JEGHAR.

7. Ikonnikov S. E. Sozdanie sistemy zashchity i avtomatizatsiya informatsionnoy bezopasnosti na ob"ektakh kriticheskoy informatsionnoy infrastruktury / S. E. Ikonnikov // Intellektual'nye transportnye sistemy: Materialy III Mezhdunarodnoy nauchno-prakticheskoy konferentsii, Moskva, 30 maya 2024 goda. – Moskva: Rossiyskiy universitet transporta (MIIT), 2024. – S. 575-578. – DOI 10.30932/9785002446094-2024-575-578. – EDN RVIGBA.

8. Metodika obespecheniya ustoychivosti funktsionirovaniya kriticheskoy informatsionnoy infrastruktury v usloviyakh informatsionnykh vozdeystviy / S. M. Klimov, S. V. Polikarpov, B. S. Ryzhov [i dr.] // Voprosy kiberbezopasnosti. – 2019. – № 6(34). – S. 37-48. – DOI 10.21681/2311-3456-2019-6-37-48. – EDN ANVHWE.

9. Smirnov G. E. Aktual'nye voprosy razvitiya teorii i praktiki audita informatsionnoy bezopasnosti ob"ektov kriticheskoy informatsionnoy infrastruktury / G. E. Smirnov, S. I. Makarenko // Problemy kompleksnoy bezopasnosti Kaspiyskogo makroregiona: Sbornik nauchnykh statey po materialam mezhdunarodnoy nauchno-prakticheskoy konferentsii, Astrakhan', 28–29 oktyabrya 2021 goda / Pod obshchey redaktsiey A.P. Romanovoy, D.A. Chernichkina. – Astrakhan': Astrakhanskiy gosudarstvennyy universitet, Izdatel'skiy dom "Astrakhanskiy universitet", 2021. – S. 148-157. – EDN MSQRDC.

10. Voevodin V. A. O probleme otsenivaniya ustoychivosti funktsionirovaniya ob"ektov kriticheskoy informatsionnoy infrastruktury dlya usloviy vozdeystviya ugroz informatsionnoy bezopasnosti / V. A. Voevodin // Radioelektronnye ustroystva i sistemy dlya infokommunikatsionnykh tekhnologiy" ("REUS-IT 2024"): Doklady Vserossiyskoy konferentsii, posvyashchennoy Dnyu radio, Moskva, 31 maya 2024 goda. – Moskva: Rossiyskoe nauchno-tekhnicheskoe obshchestvo radiotekhniki, elektroniki i svyazi im. A.S. Popova, 2024. – S. 299-304. – EDN UPBBWH.

КУШНИР Надежда Владимировна, старший преподаватель кафедры информационных систем и программирования федерального государственного бюджетного образовательного учреждения высшего образования «Кубанский государственный технологический университет». 350072, г. Краснодар, ул. Московская, д. 2. E-mail: kushnir.06@mail.ru

ЯЦКЕВИЧ Евгений Сергеевич, магистрант 2 курса федерального государственного бюджетного образовательного учреждения высшего образования «Кубанский государственный технологический университет». 350072, г. Краснодар, ул. Московская, д. 2. E-mail: es_yatskevich@internet.ru

ВЛАСЕНКО Александра Владимировна, кандидат технических наук, доцент, профессор кафедры информационной безопасности Краснодарского университета МВД России. 350005, г. Краснодар, ул. Ярославская 128. E-mail: alex_vlasenko@list.ru

КОПЦОВ Сергей Васильевич, кандидат социологических наук, полковник полиции, старший преподаватель кафедры информационной безопасности Краснодарского университета МВД России. 350005, г. Краснодар, ул. Ярославская 128. E-mail: Serega.kchr@yandex.ru

KUSHNIR Nadezhda Vladimirovna, Senior Lecturer at the Department of Information Systems and Programming of the Federal State Budgetary Educational Institution of Higher Education «Kuban State Technological University». 2 Moskovskaya St., Krasnodar, 350072. E-mail: kushnir.06@mail.ru

YATSKEVICH Evgeny Sergeevich, 2nd year Master's student at the Federal State Budgetary Educational Institution of Higher Education «Kuban State Technological University». 2 Moskovskaya St., Krasnodar, 350072. E-mail: es_yatskevich@internet.ru

VLASENKO Alexandra Vladimirovna, Candidate of Technical Sciences, Associate Professor, Professor of the Department of Information Security at the Krasnodar University of the Ministry of Internal Affairs of Russia. 128 Yaroslavskaya St., Krasnodar, 350005. E-mail: alex_vlasenko@list.ru

KOPTSOV Sergey Vasilyevich, Candidate of Sociological Sciences, Police Colonel, Senior Lecturer at the Department of Information Security of the Krasnodar University of the Ministry of Internal Affairs of Russia. 128 Yaroslavskaya St., Krasnodar, 350005. E-mail: Serega.kchr@yandex.ru

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

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

ВЕСТНИК УрФО
Безопасность в информационной сфере № 1(55) / 2025
Подписано в печать 31.03.2025. Дата выхода в свет 31.03.2025.
Формат 70×108 1/16. Печать цифровая. Усл.-печ. л. 7,79. Тираж 50 экз.
Заказ XXX/XXX.
Цена свободная.

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

Bulletin of the Ural Federal District
Security in the Sphere of Information No. 1(55) / 2025
Signed to print 31.03.2025. Date of publication of the 31.03.2025.
Format 70×108 1/16. Screen printing. Conventional printed sheet 7,79. Circulation – 50 issues.
Order XXX/XXX.
Open price.

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