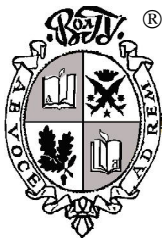
ISSN 2658-3593 (Print)
ISSN 2713-1564 (Online)



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

НБИ ТЕХНОЛОГИИ

Нано / Био / Инновационные технологии

2020
Том 14. № 3

MINISTRY OF SCIENCE AND HIGHER EDUCATION
OF THE RUSSIAN FEDERATION

NBI TECHNOLOGIES

Nano / Bio / Innovation Technologies

2020
Volume 14. No. 3

NBI TECHNOLOGIES

2020. Vol. 14. No. 3

Academic Periodical

First published in 2006

4 issues a year

Founder:
Federal State Autonomous
Educational Institution
of Higher Education
"Volgograd State University"

The journal is registered in the Federal Service for Supervision of Communications, Information Technology and Mass Media (Registration Number **ПИ № ФС77-73361** of July 24, 2018)

The journal is included into the **Russian Science Citation Index**

The journal is also included into the following Russian and international databases: **CrossRef** (USA), **DOAJ** (Sweden), **ProQuest** (USA), **Google Scholar** (USA), **JournalSeek** (USA), **OCLC WorldCat**© (USA), **SHERPA/RoMEO** (Spain), **ULRICHSWEB™ Global Serials Directory** (USA), **VINITI Database RAS** (Russia), **"CyberLeninka" Scientific Electronic Library** (Russia), **"Socionet" Information Resourses** (Russia), **IPRbooks E-Library System** (Russia), **E-Library System "University Online Library"** (Russia)

Editor of English texts *Yu.V. Chemeteva*
Making up: *Yu.A. Uskova*
Technical editing: *S.A. Astakhova, O.N. Yadykina*

Passed for printing: Dec. 22, 2020.
Date of publication: Mar. 26, 2021.
Format 60×84/8. Offset paper. Typeface Times.
Conventional printed sheets 4.3. Published pages 4.6.
Number of copies 500 (1st dublicate 1–40).
Order . «C» 44.

Open price

Address of the Printing House:
Bogdanova St, 32, 400062 Volgograd.
Postal Address:
Prosp. Universitetsky, 100, 400062 Volgograd.
Publishing House of Volgograd State University.
E-mail: izvolgu@volsu.ru

Address of the Editorial Office and the Publisher:
Prosp. Universitetsky, 100, 400062 Volgograd.
Volgograd State University.
Tel.: (8442) 46-03-68, 46-55-99. Fax: (8442) 46-18-48
E-mail: vestnik10@volsu.ru

Journal website: https://ti.jvolsu.com
English version of the website:
https://ti.jvolsu.com/index.php/en/

НБИ ТЕХНОЛОГИИ

2020. Т. 14. № 3

Научно-теоретический журнал

Основан в 2006 году

Выходит 4 раза в год

Учредитель:
Федеральное государственное автономное образовательное учреждение высшего образования «Волгоградский государственный университет»

Журнал зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (регистрационный номер **ПИ № ФС77-73361** от 24 июля 2018 г.)

Журнал включен в базу **Российского индекса научного цитирования (РИНЦ)**

Журнал также включен в следующие российские и международные базы данных: **CrossRef** (США), **DOAJ** (Швеция), **ProQuest** (США), **Google Scholar** (США), **JournalSeek** (США), **OCLC WorldCat©** (США), **SHERPA/RoMEO** (Испания), **ULRICHSWEB™ Global Serials Directory** (США), **ВИНИТИ** (Россия), **Научная электронная библиотека «КиберЛенинка»** (Россия), **Соционет** (Россия), **Электронно-библиотечная система IPRbooks** (Россия), **Электронно-библиотечная система «Университетская библиотека онлайн»** (Россия)

Редактор английских текстов *Ю.В. Чеметева*
Верстка *Ю.А. Усковой*
Техническое редактирование *С.А. Астаховой, О.Н. Ядыкиной*

Подписано в печать 22.12 2020 г.
Дата выхода в свет 26.03 2021 г.
Формат 60×84/8. Бумага офсетная. Гарнитура Таймс.
Усл. печ. л. 4,3. Уч.-изд. л. 4,6.
Тираж 500 экз. (1-й завод 1–40 экз.).
Заказ . «С» 44.

Свободная цена

Адрес типографии:
400062 г. Волгоград, ул. Богданова, 32.
Почтовый адрес:
400062 г. Волгоград, просп. Университетский, 100.
Издательство
Волгоградского государственного университета.
E-mail: izvolgu@volsu.ru

Адрес редакции и издателя:
400062 г. Волгоград, просп. Университетский, 100.
Волгоградский государственный университет.
Тел.: (8442) 46-03-68, 46-55-99. Факс: (8442) 46-18-48
E-mail: vestnik10@volsu.ru
Сайт журнала: https://ti.jvolsu.com
Англояз. сайт журнала:
https://ti.jvolsu.com/index.php/en/

СОДЕРЖАНИЕ

CONTENTS

Обращение главного редактора

Дорогие друзья, авторы и читатели нашего журнала!

В настоящее время приоритетное внимание должно быть уделено активизации инновационной деятельности по воплощению результатов научно-технических разработок в производство, развитию инновационных предприятий, созданию новых технологических процессов и перестройке на современной научно-технической основе всех отраслей промышленности и сферы обслуживания.

Достижение существенных результатов в развитии инновационной сферы среди более широкого круга предприятий в ближайшее время представляется проблематичным в связи с существованием ряда факторов, сдерживающих инновационную активность. В настоящее время идет процесс накопления инновационного потенциала. Взаимодействие технических, инженерных знаний с информационными технологиями, которого требует сегодня разработка интеллектуальных систем, с неизбежностью предполагает диалог между представителями различных научных дисциплин, междисциплинарный подход, в котором действия специалистов в рамках одной научной дисциплины дополняются исследованиями других исследовательских сообществ. Журнал «НБИ технологии» предназначен освещать широкий спектр научных проблем, связанных с решением актуальных вопросов в сфере науки, техники и инноваций.

Редакционный совет журнала приглашает всех исследователей, работающих в области разработки и внедрения инноваций, к публикации своих работ на страницах нашего журнала.

Редакционный совет и редколлегия журнала благодарят всех участников подготовки и выпуска журнала за поддержку.

И.В. Запороцкова,
доктор физико-математических наук, профессор,
директор института приоритетных технологий ВолГУ

DOI: https://doi.org/10.15688/NBIT.jvolsu.2020.3.1

УДК 681.5:005.71
ББК 32.81

СНИЖЕНИЕ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СУБЪЕКТОВ ДЕЦЕНТРАЛИЗОВАННЫХ АВТОНОМНЫХ ОРГАНИЗАЦИЙ

Юлия Сагидулловна Бахрачева

Кандидат технических наук, доцент кафедры информационной безопасности,
Волгоградский государственный университет
bakhracheva@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Арина Романовна Алеева

Студент кафедры информационной безопасности,
Волгоградский государственный университет
bakhracheva@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Целью данной работы является снижение риска информационной безопасности субъектов децентрализованных автономных организаций. Для этого была проведена разработка математической модели аудита информационной безопасности субъектов децентрализованных автономных организаций.

Ключевые слова: информационная безопасность, математическая модель, аудит информационной безопасности, децентрализованные автономные организации, Интернет.

Интернет быстро вступает в новую технологическую эру с появлением технологии блокчейн, дающая возможность обмениваться ценностями совершенно безопасно [3]. Данная технология является инструментом для появления децентрализованных автономных организаций.

Децентрализованные автономные организации (ДАО), использующие технологию распределенной бухгалтерской книги, могут потенциально улучшить корпоративное управление за счет автоматизации базовых правил. На сегодняшний день ДАО, как новый тип экономической организации, жизнеспособна и эффективна в теории, но требует от разработчиков особой тщательности в сфере безопасности от атак и случайных ошибок в коде [1; 2; 4].

Децентрализованные автономные организации состоят из субъектов, наделенных определенными правами. Действия субъектов могут привести к определенным последствиям, влияющих на стабильность ДАО. Данные организации должны отслеживать состояние системы. Для решения этого вопроса необходимо проводить аудит информационной безопасности, позволяющий дать количественную и качественную оценки состояния информационной безопасности.

Целью данной работы является снижение риска информационной безопасности субъектов децентрализованных автономных организаций. Для этого была проведена разработка математической модели аудита информационной безопасности субъектов децентрализованных автономных организаций.

Проект модели выполнен в соответствии с методологией функционального моделирования IDEF0, предназначенной для формализации и описания процесса проведения аудита информационной безопасности субъектов децентрализованных автономных организаций. Контекстная IDEF0 – диаграмма процесса проведения аудита представлена на рисунке 1.

На функциональный блок «Аудит информационной безопасности субъектов децентрализованных автономных организаций» воздействуют:

1) Входные данные – информация о децентрализованных автономных организациях.

2) Управляющая информация, в качестве которой выступают – список возможных угроз, существующие данные, математическая модель и меры предотвращения угроз.

3) Механизмами, необходимыми для повышения защищенности, являются программное средство и пользователь.

4) В результате данных воздействий на выходе функции результат – программный комплекс, способный проводить аудит ИБ субъектов ДАО.

При декомпозиции функционального блока выделены его составляющие:

1) Определение функционала планируемой ДАО.

2) Обрабатывание данных существующей ДАО.

3) Изъятие данных существующей ДАО.

4) Расчет показателя ИБ ДАО и оценки рисков.

5) Определение мер предотвращения угроз ИБ ДАО.

6) Снижение риска.

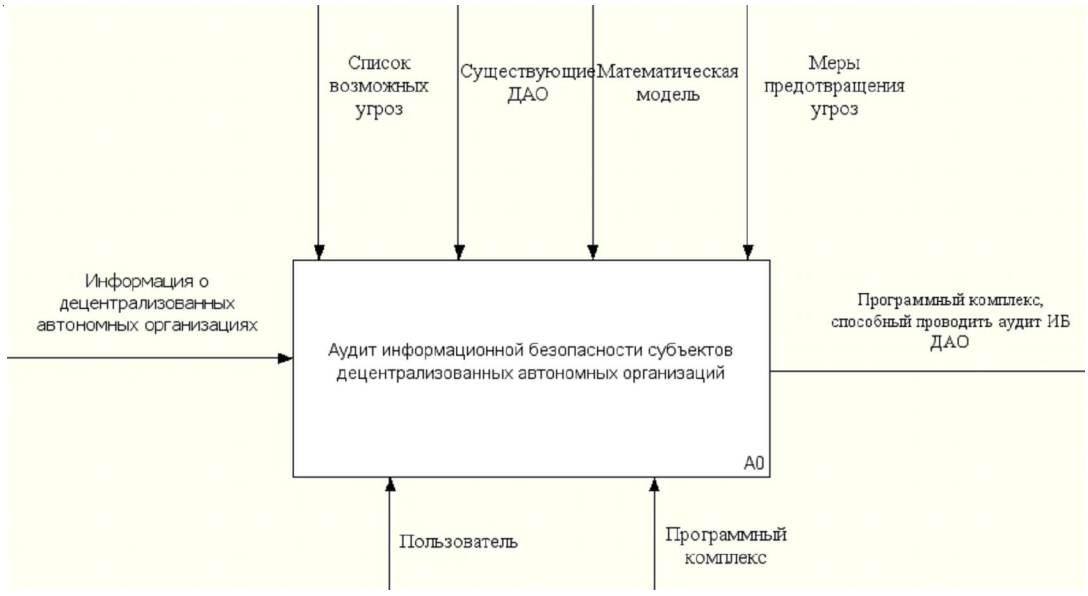


Рис. 1. Контекстная IDEF0 – процесса проведения аудита ИБ субъектов ДАО

На блок модуля «определение функционала планируемой ДАО» воздействуют:

1) Входные данные – информация о децентрализованных автономных организациях.

2) Управляющая информация – список возможных угроз.

3) Механизмами являются: программный комплекс и пользователь.

4) В результате данных воздействий на выходе функции результат – входные данные для расчета.

На блок «обрабатывание данных существующей ДАО» воздействуют:

1) Входные данные – заполнение полученными данными о существующей ДАО.

2) Управляющая информация – существующие ДАО.

3) Механизмом является программный комплекс.

4) В результате данных воздействий на выходе функции результат – входные данные для расчета.

На блок «изъятие данных существующей ДАО» воздействуют:

1) Входные данные – информация о децентрализованных автономных организациях.

2) Управляющая информация – существующие ДАО.

3) Механизмами являются: программный комплекс и пользователь.

4) В результате данных воздействий на выходе функции результат – заполнение полученными данными о существующей ДАО.

На блок «расчет показателя ИБ ДАО и оценки рисков» воздействуют:

1) Входные данные – входные данные для расчета.

2) Управляющая информация – математическая модель.

3) Механизмами являются: программный комплекс и пользователь.

4) В результате данных воздействий на выходе функции результат – результаты оценок рисков и показателя ИБ ДАО.

На блок «определение мер предотвращения угроз ИБ ДАО» воздействуют:

1) Входные данные – результаты оценок рисков и показателя ИБ ДАО.

2) Управляющая информация – список возможных угроз.

3) Механизмом является программный комплекс.

4) В результате данных воздействий на выходе функции результат – применение мер защиты.

На блок «снижение риска» воздействуют:

1) Входные данные – применение мер защиты.

2) Управляющая информация – меры предотвращения угроз.

3) Механизмами являются: программный комплекс и пользователь.

4) В результате данных воздействий на выходе функции результат – программный комплекс, способный проводить аудит ИБ ДАО.

Далее была проведена разработка архитектуры программного комплекса аудита информационной безопасности субъектов децентрализованных автономных организаций. На рисунке 2 представлена архитектура ДАО.

Основными компонентами разработанной архитектуры являются:

– Интерфейс пользователя.

– Модуль идентификации ДАО.

– Модуль функционирования смарт-контрактов.

– Модуль разделения капитала и силы голосования.

– Модуль реализации голосования.

– Обработка данных результатов функционирования.

К модулю обработки данных результатов функционирования дополняется модуль аудита ИБ ДАО, который в свою очередь имеет другую архитектуру (см. рис. 3).

Основными компонентами разработанной архитектуры являются:

– Пользовательский интерфейс.

– Модуль определения функционала планируемой ДАО.

– Модуль изъятия данных существующей ДАО.

– Модуль обработки данных, существующей ДАО.

– Модуль расчета показателя ИБ ДАО и оценки рисков.

– Модуль определения мер предотвращения угроз ИБ.

Пользовательский интерфейс имеет графический вид и предназначен для ввода дан-

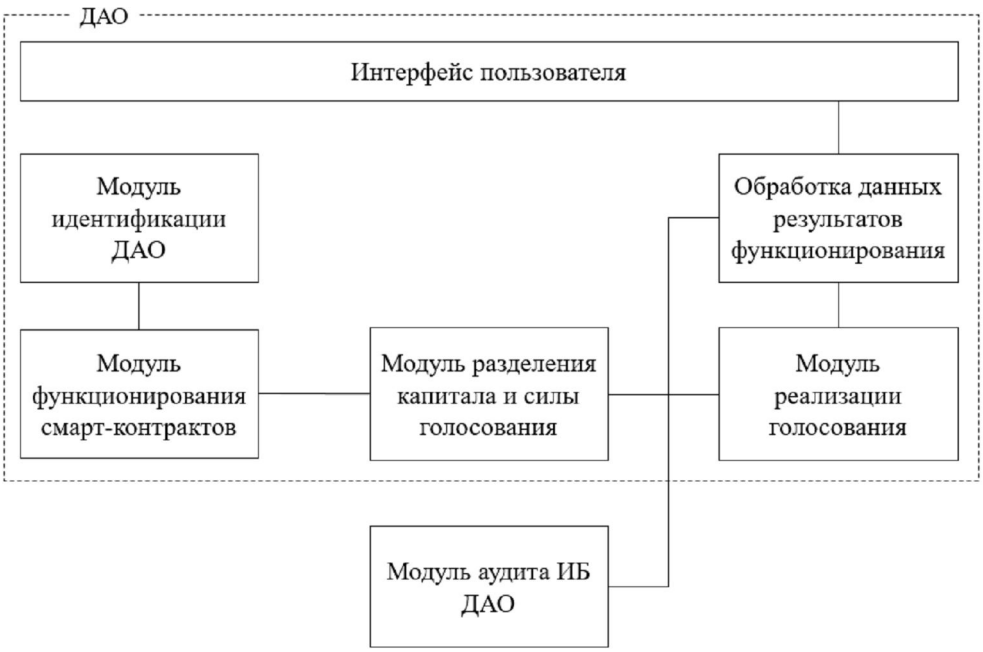


Рис. 2. Архитектура ДАО

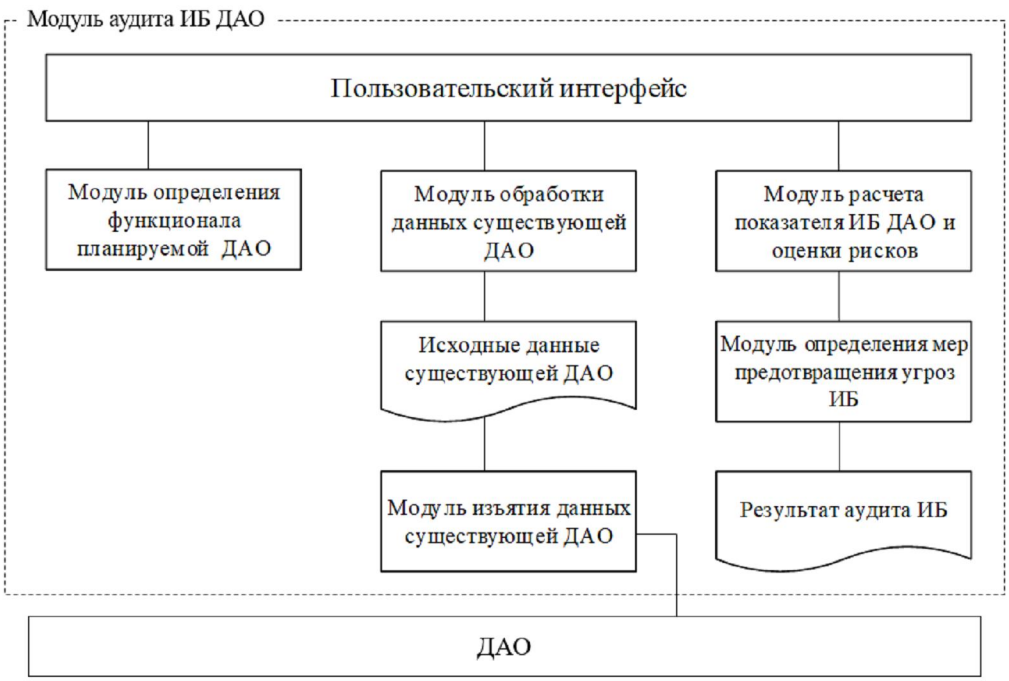


Рис. 3. Архитектура программного комплексааудита ИБ субъектов ДАО

ных, вывода результатов и организации взаимодействия пользователя с программой.

Модуль определения функционала планируемой ДАО предназначен для ввода данных и организации взаимодействия пользователя с программой.

Модуль изъятия данных существующей ДАО позволяет извлекать и преобразовывать информацию из ДАО для ее дальнейшего использования в программном комплексе.

Исходные данные существующей ДАО содержат в себе данные о всех параметрах ДАО и их функционала.

Модуль обработки данных, существующей ДАО, позволяет обработать информацию

и автоматически заполнить поля данных программного комплекса.

Модуль расчета показателя ИБ ДАО и оценки рисков рассчитывает данные по угрозам для определения качественной или количественной оценки рисков, а также значение показателя ИБ ДАО.

Модуль определения мер предотвращения угроз ИБ предназначен для подбора меры предотвращения в соответствии с угрозой.

Результат аудита ИБ содержит отчет об выявленных угрозах, оценку рисков и меры предотвращения.

На основании разработанной архитектуры программного комплекса разработан пользовательский интерфейс (рис. 4).

Данный пользовательский интерфейс содержит в себе:

– Область выбора вида ДАО для проведения аудита.

– Область выбора функционала ДАО.

– Область заполнения доступных вкладок по функционалу ДАО.

– Кнопки «Выбрать файл», «Оценить риски и показатель ИБ ДАО» и «Сохранить и показать отчет» для взаимодействия с данными, введенными в различные области на данном интерфейсе.

На панели интерфейса имеется:

– Кнопки выбора вида ДАО для проведения аудита ИБ, которые позволяют выбрать вид ДАО для дальнейшей работы.

– Кнопка выбора файла с данными, существующей ДАО, позволяющая загрузить файл с информацией о ДАО.

– Кнопки выбора функционала в ДАО, в которых пользователь выбирает функционал ДАО в соответствии с параметрами ДАО.

– Кнопки выбранного функционала ДАО включают в себя доступный функционал, в каждой вкладке которого вводятся данные для дальнейших расчетов.

– Поля данных для заполнения в соответствии с ДАО позволяет заполнить поля для расчетов по формулам.

– Кнопка для проведения оценки риска рассчитывает оценки рисков, которые могут быть низкими, средними или высокими, также подбирает меры предотвращения.

– Кнопка для создания отчета по аудиту ИБ формирует документ, в котором будет

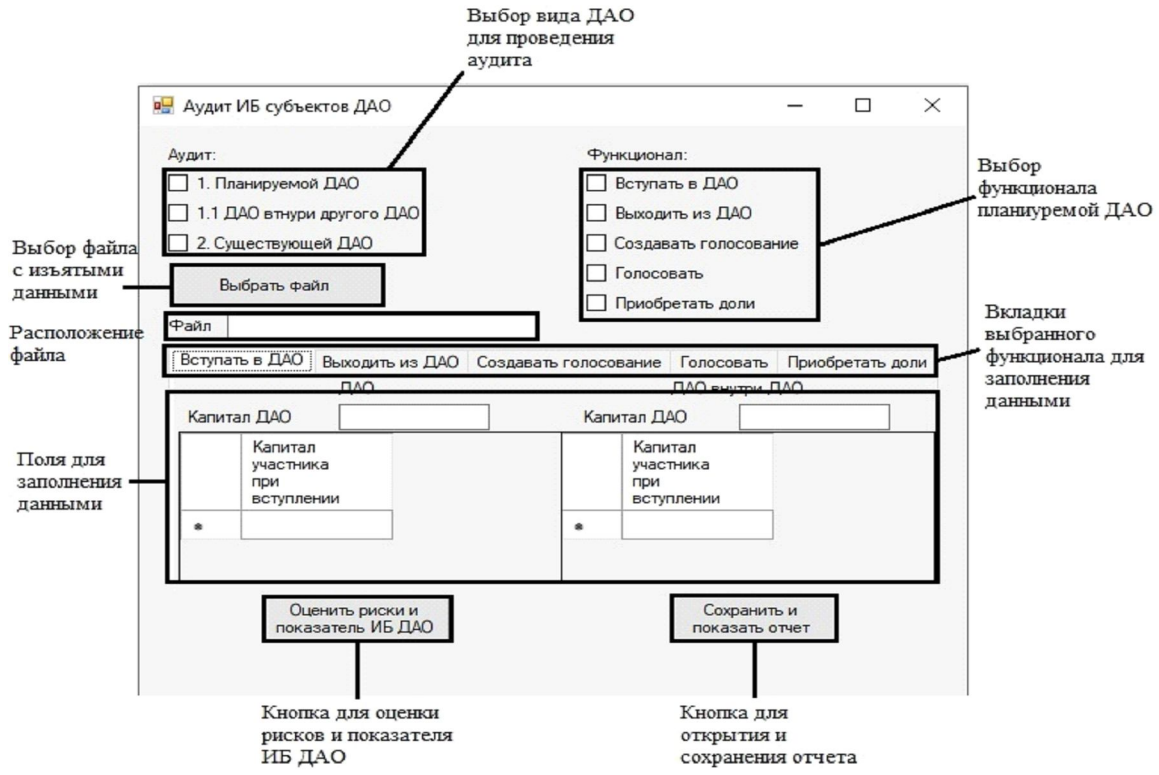


Рис. 4. Пользовательский интерфейс программного комплекса аудита ИБ субъектов ДАО

перечень выявленных угроз, оценка рисков, показатель ИБ ДАО и меры предотвращения.

Далее были проведены экспериментальные исследования работы разработанного программного комплекса. Было показано, что остаточный риск уменьшился на 2,5, а процент снижения риска уменьшился на 42,8 %.

СПИСОК ЛИТЕРАТУРЫ

1. Antonopoulos, A. M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies / A. M. Antonopoulos. – Sebastopol, CA, USA : O'Reilly Media, 2014. – 270 p.

2. Ethereum white paper / V. Buterin [et al.] // GitHub repository. – 2013. – Vol. 1. – P. 22–23.

3. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system / S. Nakamoto. – Manubot, 2019. – Electronic text data. – Mode of access: https://git.dhimmel.com/bitcoin-whitepaper/ (date of access: 27.09.2020).

4. Theory and praxis of DAOs. How can DAOs be conceptualized and classified? – 2019. – Electronic text data. – Mode of access: https://research.binance.com/analysis/dao-theory (date of access: 26.09.2020).

REFERENCES

1. Antonopoulos A.M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Sebastopol, CA, USA, O'Reilly Media, 2014. 270 p.

2. Buterin V. et al. Ethereum white paper. *GitHub repository*, 2013, vol. 1, pp. 22-23.

3. Nakamoto S. *Bitcoin: A peer-to-peer electronic cash system*. Manubot, 2019. URL: https://git.dhimmel.com/bitcoin-whitepaper/ (accessed 27 September 2020).

4. *Theory and praxis of DAOs. How can DAOs be conceptualized and classified?* 2019. URL: https://research.binance.com/analysis/dao-theory (accessed 26 September 2020).

REDUCING THE RISK OF INFORMATION SECURITY OF SUBJECTS OF DECENTRALIZED AUTONOMOUS ORGANIZATIONS

Yulia S. Bahracheva

Candidate of Sciences (Engineering), Associate Professor, Department of Information Security,
Volgograd State University
bakhracheva@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Arina R. Aleeva

Student, Department of Information Security,
Volgograd State University
bakhracheva@volsu.ru 100
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. The purpose of this work is to reduce the risk of information security of subjects of decentralized autonomous organizations. For this purpose, a mathematical model of the audit of information security of subjects of decentralized autonomous organizations was developed.

Key words: information security, mathematical model, information security audit, decentralized autonomous organizations, Internet.

DOI: https://doi.org/10.15688/NBIT.jvolsu.2020.3.2

УДК 004.9:550.34.01
ББК 32.972.53

РАЗРАБОТКА ФОРМАЛЬНОЙ МОДЕЛИ ИССЛЕДОВАНИЯ МЕТОДОВ ОПРЕДЕЛЕНИЯ НАДЕЖНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Александр Алексеевич Бочкарев

Студент кафедры информационной безопасности,
Волгоградский государственный университет
bochkarev_10@mail.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Алексей Александрович Бабенко

Кандидат педагогических наук, доцент кафедры информационной безопасности,
Волгоградский государственный университет
ba_benko@mail.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Рассмотрены понятия информационной системы и ее надежности. Проанализированы модели и методы определения надежности информационных систем. Определены критерии для разработки формальной модели исследования методов оценки надежности информационных систем. Разработана формальная модель для исследования методов определения надежности информационных систем.

Ключевые слова: информационная система, надежность, формальная модель, анализ методов, разработка модели, группы критериев, количественная оценка, качественная оценка.

Введение

Состояние надежности является основным показателем стабильного функционирования информационной системы. Оценка надежности – это комплексный показатель, который складывается из четырех групп свойств, а именно: долговечность, безотказность, ремонтопригодность и комплексные показатели. В свою очередь, свойства надежности имеют в составе, показатели каждого из свойств. Так, например, в ГОСТ 27.002-89 [2; 8] определены основные показатели надежности, к этим показателям относятся: время безотказной работы, среднее время на отказ, интенсивность отказов, срок службы и так далее.Именно на основе этих показателей и дается оценка надежности, используемой или проектируемой информационной системы.

Стабильное функционирование информационных систем во многом зависит от надежной работы технических составляющих системы как физических, так и программных. Основаниями, которые полагают усиленный интерес к проблемам определения надежности ИС, являются: повышение сложности аппаратной части ИС и возникновению высокопроизводительных информационных систем;

замедленный рост уровня надежности составляющих ее частей; повышение значимости реализуемой аппаратурной работой; сложности условий использования и т. д.

Для оценки надежности на практике используют вероятностные, динамические, прогнозные и статические модели определения надежности информационных систем. Каждый из этих методов в основу определения своей оценки надежности использует как раз представленные показатели надежности.

Анализ моделей определения надежности информационных систем

Выделяют следующие группы моделей определения надежности информационных систем:

1.Вероятностные динамические модели определения надежности информационных систем;

1.1. Модель Джелинского-Моранды;

1.2. Модель Муса;

1.3. Модель Шика – Волвертона;

2. Вероятностные статистические модели определения надежности информационных систем;

2.1. Модель Монте-Карло;

2.2. Модель Миллса.

Вероятностные динамические модели определения надежности информационных систем собирают статистические данные об ошибках, которые обнаруживаются в процессе тестирования или функционирование информационной системы [5; 7].

В настоящее время одна из наиболее используемых моделей оценки надежности, которая относится к вероятностным динамическим моделям, является модель Джелинского-Моранды [1]. Данная модель основана на времени между обнаружением ошибок на экспоненциальном распределении в процессе тестирования или использования информационной системы со значением пропорциональному общему числу найденных ошибок в системе. Ошибки, которые обнаружила модель равновероятные, то есть не зависят друг от друга, из этого следует, что ошибки не подразделяются по степеням важности. Количество обнаруженных ошибок на определенном интервале времени линейно зависит от общего числа ошибок, оставшихся в системе [3].

Еще одна из часто используемых вероятностных динамических моделей, модель Муса. Для своего функционирования модель использует показатель надежности, связанный со средней наработкой на отказ. Во время очередного тестирования информационной системы, устанавливается время до момента обнаружения отказа. При этом не каждая ошибка в выполнении программы может вызнать отказ, поэтому допускаетсядо появления отказа более одной ошибки. Модель Муса относят к моделям с нескончаемым временим, которые имеют два вида. В первом типе моделей рассматривается эффективное время – время не отказной работы во время использования. Во втором типе моделей рассматривается итоговое время работоспособности, при этом проводится оценка надежности, учитывающее время с момента начала тестирования и до определения самой надежности.

Модель Шика – Волвертона также относится к динамическим вероятностным моделям. Суть данной модели в том, что вероятность возникновения ошибок пропорционально растет со временем использованием и также с начала момента тестирования информационной системы. При этом ошибки исправляются сразу же с момента их обнаружения. Время ожидания каждый ошибки в этой модели не является главным критерием, указывается временной интервал, для того чтобы определить число ошибок на нем [6].

Вероятностные статистические модели определения надежности информационных систем отличаются от динамических тем, что в них не вводят интервал, на котором обнаруживается ошибки в информационной системе от времени выполнении тестирования [7].

Модель Монте-Карло основывается на сравнении вероятных значениях случайной величины, с распределением данной вероятности. При этом собираются статистические данные о процессах, которые происходят в информационной системе с учетом факторов внешней среды. Недостатком этого метода является то, чтовозрастает сложность, а соответственно усложняется схема оценки надежности в процессе перехода

от возможных отказов к значениям наработки на отказ [9].

Модель Миллса используется для определения оценки надежности информационной системы. Перед началом тестирования вводят известное количество ошибок, и только после этого предлагается проводить поиск имеющихся ошибок. Программа считается надежной, если в ней не было выявлено ни одной ошибки. Сотрудник, проводящий оценку надежности, не знает о наличие так называемых «искусственных ошибок», поэтому все найденные ошибки, как и в модели Джелинского – Моранды имеют одинаковую степень важности [6].

С целью выбора наиболее эффективной модели определения надежности информационных систем сформулируем критерии для их оценки.

Анализ критериев для разработки формальной модели исследования методов определения надежности информационных систем

Модели анализа методов определения надежности информационных систем обсуждаются с позиции оценки критериев на начальных стадиях проектирования, точности этих критериев, связи и влияния оценок надежности и трудоемкости.

Метод экспертных оценок состоит в поиске и сборе информации с помощью опроса специалистов, при этом достоверность полученных данных складывается с уровнем знаний и справедливостью экспертных оценок.

Выделим критерии для разработки формальной модели исследования методов определения надежности информационных систем (табл. 1):

1. Простота использования –насколько комфортно работать с программнымобеспечением для определения надежности информационных системсотруднику не имеющим специальной квалификации и насколько легко он может обучиться.

2. Возможность автоматизации – насколько программное обеспечение может использоваться в получения оценки надежности информационной системы без участия людей, либо во многом уменьшает степень их участия.

3. Подходит для сложных систем – насколько метод определения надежности информационной системы подходит для систем, которые являются сложными.

4. Полнота охвата показателей надежности – какое количество показателей надежности в соответствии с «ГОСТ 27.002-89. Надежность в технике», охватывает метод определения надежности информационной системы.

5. Цена – стоимость определения оценки надежности информационных систем с помощью указанногометода.

6. Стоимость одного года обслуживания – стоимость метода определение оценки надежности информационных систем за один год обслуживания.

7. Эффективность – соотношение между достигнутым результатом и использованными ресурсами в определение оценки надежности информационной системы.

8. Сопровождаемость – критерий, который позволяют максимально уменьшить затраты по изменению устранений ошибок в методеи по его модификации в соответствии с изменяющимися потребностями пользовате-

Таблица 1

Критерии оценки моделей определения надежности

Обозначение	Название
К1.1	Полнота охвата показателей надежности
К1.2	Эффективность
К1.3	Стойкость к отказам
К2.1	Возможность автоматизации
К2.2	Подходит для сложных систем
К3.1	Квалификация исполнителя
К3.2	Сопровождаемость
К3.3	Простота реализации
К4.1	Цена
К4.2	Стоимость одного года обслуживания

лей в определении оценки надежности информационной системы.

9. Квалификация исполнителя – уровень качества знаний, подготовки, квалификации сотрудников, использующих программное средство для определения оценки надежности информационной системы.

10. Стойкость к отказам – критерий программного обеспечения в формировании оценки надежности информационной системы в момент обнаружения ошибок или отказов сохранять прежнюю работоспособность.

Формальная модель исследования методов определения надежности информационных систем

Для исследования методов определения надежности информационных систем предлагается разработать формальную модель, которая будет функционировать на основе частных критериев представленных выше (см. табл. 1) из каждой четырех групп $K = \{K_1, K_2, K_3, K_4,\}$.

$$K_{ij} = \begin{cases} 0.1, \text{если у критерия выбрана} \\ \text{качественная оценка – низкая} \\ 0.2, \text{если у критерия выбрана} \\ \text{качественная оценка – средняя} \\ 0.3, \text{если у критерия выбрана} \\ \text{качественная оценка – высокая} \end{cases} \quad (1)$$

$$K_{ij} = \begin{cases} 0, \text{если у критерия выбрана} \\ \text{качественная оценка – нет} \\ 0.5, \text{если у критерия выбрана} \\ \text{качественная оценка – да} \end{cases} \quad (2)$$

Идеальной модели оценки надежности соответствует вектор K^*, в котором все значения критериев равны единице. Для оценки модели вводится скалярная величина, равная метрике Манхэттена, расстоянию между наилучшим вектором K^* и вектором критериев, полученным для каждой оцениваемой модели:

$$K^i = \left(K_1^i, K_2^i, K_3^i, K_4^i,\right) \quad (3)$$

Предлагается использовать метрику Манхэттена, так как критерии оценки моделей определения надежности K_j^i не похожи по типу. Предложенная метрика позволяет проверить близость двух векторов:

$$d^i = \sum_{j=1}^{4} \left| K_j^* - K_j^i \right| . \quad (4)$$

Метод, для которого расстояние d^i до наилучшего вектора окажется наименьшим, можно считать наиболее эффективным для оценки надежности информационной системы.

Предложенная формальная модель позволяет выбрать наиболее эффективный метод оценки надежности информационных систем.

Для получения экспертных оценок определения надежности информационных систем выделены следующие задачи и методы их решения:

1) для подбора экспертов использовался документальный метод;

2) для проведения опроса экспертов использовался метод Дельфы;

3) для обработки результатов опроса использовалась проверка гипотезы согласованности мнений специалистов.

Обработка результатов экспертизы представляет собой трудоемкий процесс, следовательно, целесообразно использовать программы, реализующие алгоритмы обработки результатов экспертного оценивания.

Заключение

В таблице 2 приведены качественные значения критериев для выделенных методов определения надежности информационных систем и количественные результаты исследования с помощью разработанной формальной модели.

В результате проведенных экспериментов наиболее эффективнымметодом оценки надежности является модель Джелинского-Моранды. Оценка надежности информационной системы проводилась исходя из личных потребностей специалиста к модели, проводившего оценку каждой модели, поэтому выбор метода является субъективным и строится из потребностей, которые в свою очередь диктует руководство или сотрудники, проектирующие информационную систему [4].

Таблица 2

Результаты равнениеметодовнадежности информационных системпо критериям

Название критерия	Модель Джелинского-Моранды	Модель Муса	Модель Шика – Волвертона	Модель Монте-Карло	Модель Миллса
Простота использования	Высокая	Высокая	Средняя	Низкая	Низкая
Возможность автоматизации	Да	Нет	Нет	Да	Да
Подходит для сложных систем	Да	Да	Нет	Нет	Нет
Полнота охвата показателей надежности	Средняя	Низкая	Низкая	Низкая	Средняя
Цена	Средняя	Средняя	Средняя	Высокая	Средняя
Стоимость одного года обслуживания	Низкая	Низкая	Низкая	Высокая	Средняя
Эффективность	Высокая	Средняя	Средняя	Низкая	Средняя
Сопровождаемость	Низкая	Средняя	Высокая	Низкая	Низкая
Квалификация исполнителя	Средняя	Низкая	Средняя	Высокая	Высокая
Стойкость к отказам	Высокая	Высокая	Средняя	Высокая	Высокая
Итог	2,7	2	1,5	2,1	2,1

СПИСОК ЛИТЕРАТУРЫ

1. Василенко, Н. В. Модели оценки надежности программного обеспечения / Н. В. Василенко, В. А. Макаров // Вестник Новгородского государственного университета. – 2004. – С. 126–132.

2. ГОСТ Р 27.002–2009. Надежность в технике. Термины и определения. – М. : Изд-во стандартов, 2009.

3. Зубкова, Т. М. Технология разработки программного обеспечения : учеб. пособие / Т. М. Зубкова. – СПб. : Лань, 2019. – 324 с.

4. Козунова, С. С. Модель профиля угроз информационной безопасности корпоративной информационной системы / С. С. Козунова, А. А. Бабенко / / НБИ технологии. – 2018. – Т. 12, № 1. – С. 6–11.

5. Крутиков, Д. И. Вероятностная модель оценки надежности информационных систем / Д. И. Крутиков, А. А. Бабенко // IT-технологии: развитие и приложения : сб. докл. – Владикавказ : Северо-Кавказский горно-металлургический институт, 2018. – С. 129–134.

6. Мальков, М. В. О надежности информационных систем : монография / М. В. Мальков. – Кольский : Изд-во Кольский НЦ РАН, 2012. – 58 с.

7. Модели и методы исследования информационных систем : монография / А. Д. Хомоненко, А. Г. Басыров, В. П. Бубнов [и др.] ; под ред. А. Д. Хомоненко. – СПб. : Лань, 2019. – 204 с.

8. Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 г. № 149-ФЗ. – Доступ из справ.-правовой системы «Консультант Плюс».

9. Хунов, Т. Х. Анализ моделей прогнозирования надежности программных средств / Т. Х. Хунов. – М. : НИУ Высшая школа экономики : МИЭМ, 2016. – 5 с.

REFERENCES

1. Vasilenko N.V., Makarov V.A. Modeli otsenki nadezhnosti programmnogo obespecheniya. *Vestnik Novgorodskogo gosudarstvennogo universiteta*, 2004, pp. 126-132.

2. *GOST R 27.002-2009. Nadezhnost v tekhnike. Terminy i opredeleniya*. Moscow, Izd-vo standartov, 2009.

3. Zubkova T.M. *Tekhnologiya razrabotki programmnogo obespecheniya: ucheb. posobiye*. Saint Petersburg, Lan Publ., 2019. 324 p.

4. Kozunova S.S., Babenko A.A. Model profilya ugroz informatsionnoy bezopasnosti korporativnoy informatsionnoy sistemy. *NBI tekhnologii*, 2018, vol. 12, no. 1, pp. 6-11.

5. Krutikov D.I., Babenko A.A. Veroyatnostnaya model otsenki nadezhnosti informatsionnykh sistem. *IT-Tekhnologii: razvitiye i prilozheniya: sb. dokl*. Vladikavkaz, Severo-Kavkazskiy gorno-metallurgicheskiy institut, 2018, pp. 129-134.

6. Malkov M.V. *O nadezhnosti informatsionnykh sistem: monografiya*. Kolskiy, Izd-vo Kolskiy NTs RAN, 2012. 58 p.

7. Khomonenko A.D., Basyrov A.G., Bubnov V.P., Khomonenko A.D., ed. *Modeli i metody issledovaniya informatsionnykh sistem: monografiya*. Saint Petersburg, Lan Publ., 2019. 204 p.

8. Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii: feder. zakon ot 27 iyulya 2006 g. № 149-FZ. *Access from Reference Legal System "ConsultantPlus"*.

9. Khunov T.Kh. *Analiz modeley prognozirovaniya nadezhnosti programmnykh sredstv*. Moscow, NIU Vysshaya shkola ekonomiki, MIEM, 2016. 5 p.

DEVELOPMENT OF A FORMAL MODEL OF THE RESEARCH OF METHODS FOR DETERMINING THE RELIABILITY OF INFORMATION SYSTEMS

Alexandr A. Bochkarev

Student, Department of Information Security,
Volgograd State University
bochkarev_10@mail.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Aleksey A. Babenko

Candidate of Sciences (Pedagogy), Associate Professor, Department of Information Security,
Volgograd State University
ba_benko@mail.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. The state of reliability is the main indicator of the stable functioning of the information system. Reliability assessment is a complex indicator that consists of four groups of properties, namely: durability, reliability, maintainability and complex indicators. In turn, the reliability properties are composed of indicators of each of the properties. It is on the basis of these indicators that the reliability of the information system used or designed. The stable functioning of information systems largely depends on the reliable operation of technical components of the system, both physical and software. The reasons that suggest an increased interest in the problems of determining the reliability of information systems are: increasing the complexity of the hardware of information systems and the emergence of high-performance information systems; slow growth in the level of reliability of its components; increasing the significance of the hardware work implemented; complexity of the conditions of use, etc. In practice, probabilistic, dynamic, predictive, and static models for determining the reliability of information systems are used to assess reliability. Each of these methods uses the presented reliability indicators as the basis for determining its reliability assessment. The concepts of information system and reliability are presented. Models and methods for determining the reliability of information systems are analysed. Criteria for the development of a formal model of research methods for evaluating the reliability of information systems are defined. A formal model has been developed for the study of methods for determining the reliability of information systems.

Key words: information system, reliability, formal model, method analysis, model development, criteria groups, quantitative assessment, qualitative assessment.

DOI: https://doi.org/10.15688/NBIT.jvolsu.2020.3.3

УДК 681.5:004.056
ББК 32.81

МЕТОДЫ РАЗРАБОТКИ РЕКОМЕНДАЦИЙ ДЛЯ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Наталья Алексеевна Головачева

Старший преподаватель кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В работе реализована математическая модель оценки защищенности информационной системы на основе выбранных методов. Сформирована архитектура программного комплекса оценки защищенности информационной системы.

Ключевые слова: информационная безопасность, математическая модель, метод экспертных оценок, оценка защищенности, повышение защищенности.

С появлением информационных технологий широкое применение в организациях и на предприятиях получили информационные системы (ИС). Применение ИС позволяет оптимизировать трудовые ресурсы, автоматизировать полностью или частично бизнес-процессы. Однако применение ИС требует развитие системы информационной безопасность для минимизации злоумышленных воздействий. Для снижения вероятности реализации злоумышленных воздействий существует большое количество программных и программно–аппаратных средств защиты информации. Сложность организации вычислительных сред, распределенность компонентов информационных систем усложняет процесс создания и конфигурирования систем защиты, при этом количество угроз нарушения информационной безопасности (ИБ) ежегодно увеличиваются. Для своевременного реагирования на инциденты ИБ, в том числе и на атаки, необходимо применение средств оценки защищенности ИС для снижения рисков нарушения защищенности. Статистика InfoWath, показывает тенденцию роста различного рода атак, как со стороны внешнего злоумышленника, так и со стороны внутреннего. Следовательно, одной из важнейших задач является корректное определение защищенности ИС [1–3].

Целью данной работы является повышение защищенности информационной системы за счет оценки защищенности ИС.

Для достижения данной цели был определен список методов оценки защищенности ИС, а именно:

– метод экспертных оценок,

– метод оценки защищенности информации от несанкционированного доступа (НСД).

Метод экспертных оценок основывается на взаимодействии работы специалистов (экспертов), получении и обработки сложившихся мнений проведенных экспертов по возникшим вопросам. Экспертные решения формируются с целью подготовки информации для принятия решений о уровня защищенности системы.

Для проведения экспертной оценки необходимо сформировать множество оцениваемых компонентов ИС (1):

$$IS = \{k_1, \ldots\ldots, k_n\}, \quad (1)$$

где IS – множество оцениваемых компонентов ИС; k_n – компоненты ИС; n – количество компонентов ИС.

Далее необходимо определить события безопасности (2), которые могут свидетельствовать о реализации угрозы (3):

$$S = \{s_1, \ldots\ldots, s_n\}, \quad (2)$$

где S – множество совершаемых событий в ИС; s_n – события ИС; n – количество событий в ИС.

$$U = \{u_1 \ldots\ldots, u_m\}, \quad (3)$$

где U – множество актуальных угроз; u_m и $m \in N$ – количество угроз.

В зависимости от сгенерированных в ИС событий безопасности определяют возможность реализации той или иной угрозы. Формализация данного процесса представлена в формуле (4):

$$U = \begin{cases} U_1 = (S_1, S_4) \\ U_2 = (S_4, S_7) \\ U_3 = (S_4, S_7) \\ U_4 = (S_1) \\ U_5 = (S_2, S_8) \\ U_6 = (S_3, S_5, S_6) \end{cases}, \quad (4)$$

где U – множество актуальных угроз; S_1 – вход учетной записи в системы; S_2 – управление учетными записями в системе; S_3 – события маршрутизации и удаленного доступа; S_4 – событие доступа к объекту системы; S_5 – изменение политики системы; S_6 – использование субъектом особых привилегий; S_7 – функционирование процессов системы; S_8 – события входа субъектов в систему; U_1 – угрозы утечки; U_2 – угрозы искажения; U_3 – угрозы утраты; U_4 – угрозы блокирования; U_5 – угрозы взлома; U_6 – угрозы злоупотребления.

После этого следует для каждой угрозы U_i из набора актуальных угроз U определить возможные исходы реализации угроз I_{ij} или другими словами риски, которые зависят от вероятности реализации угрозы A_{ij} и Y_{il} ущерба Y_{il} (5) (см. таблицу):

$$I_{ij} = A_{ij} * Y_{il}, \quad (5)$$

где I_{ij} – риск реализации угрозы i-й угрозы для j-го компонента; A_{ij} – вероятность реализации i-й угрозы для j-го компонента; Y_{il} – ущерб от реализации от i-й угрозы для j-го компонента ИС.

Вероятности реализации оценивается следующим образом:

– маловероятно [0;0,2),
– низкая (0,2;0,4],
– средняя (0,4;0,5],
– выше среднего (0,5;0,8],
– высокая [0,8;1).

В связи с тем, что уровни предприятий различны, соответственно и ущерб будет иметь относительную количественную оценку. Распределение количественных оценок в соответствии с качественными значениями уровня ущерба приведено ниже:

– отсутствует [0;0,2),
– низкий (0,2;0,4],
– средний (0,4;0,5],
– выше среднего (0,5;0,8],
– высокий [0,8;1).

Возможные исходы реализации угрозы

I_i	Вероятность реализации угрозы (A_{ij})	Ущерб от реализации угрозы (Y_{il})
1	Маловероятно	Отсутствует
2	Маловероятно	Низкое
3	Средняя	Низкое
4	Средняя	Среднее
5	Выше среднего	Среднее
6	Выше среднего	Выше среднего
7	Выше среднего	Среднее
8	Выше среднего	Выше среднего
9	Высокая	Выше среднего
10	Высокая	Высокое

Далее рассчитывается сумма рисков реализации *i*-х угроз для *j*-го компонента (6):

$$E_{ij} = \sum_{i=1}^{n} I_{ji}, \quad (6)$$

где E_{ij} – сумма рисков от реализации угроз для *j*-го компонента; I_{ij} – возможные риски реализации *i*-й угрозы для *j*-го компонента ИС.

Суммарная оценка защищенности ИС имеет вид (7):

$$Z = \sum_{i=1}^{n} E_{ij}, \quad (7)$$

где E_{ij} – сумма возможных риски реализации *i*-х угроз для *j*-го компонента; Z – суммарная оценка защищенности ИС.

Качественная оценка защищенности ИС O_z определяется (8):

$$O_z = \begin{cases} \text{если } Z \in (40;90] - \textit{не защищена;} \\ \text{если } Z \in (20;40] - \textit{менее половины} \\ \textit{компонентов не защищены;} \\ \text{если } Z \in (10;20] - \textit{более половины} \\ \textit{компонентов защищены;} \\ \text{если } Z \in [0;10) \textit{ защищена.} \end{cases}, \quad (8)$$

где O_z – оценка защищенности ИС.

По результатам определения оценки защищенности ИС формируются рекомендации по улучшению защищенности ИС.

Рекомендации по повышению уровня защищенности при нарушении свойств безопасности информационного актива (конфиденциальность):

– рекомендуется шифрование конфиденциальной информации;

– рекомендуется настройка встроенных средств защиты ОС;

– рекомендуется установка и настройка СЗИ от НСД;

– рекомендуется установить и настроить системы аутентификации пользователей.

Рекомендации по повышению уровня защищенности при нарушении свойств безопасности информационного актива (целостность):

– рекомендуется шифрование информации;

– рекомендуется использование электронно-цифровой подписи;

– рекомендуется установка и настройка СЗИ от НСД;

– рекомендуется настройка встроенных средства защиты ОС.

Рекомендации по повышению уровня защищенности при нарушении свойств безопасности информационного актива (доступность):

– рекомендуется настройка встроенных средств защиты ОС;

– рекомендуется установка и настройка СЗИ от НСД;

– рекомендуется создание резервирования аппаратного обеспечения;

– рекомендуется резервирование информации.

Архитектура программного комплекса представлена на рисунке.

Данная архитектура состоит из следующих модулей:

– пользовательский интерфейс;

– модуль управления;

– модуль подключения к ИС;

– модуль сбора исходных данных;

– модуль оценки защищенности ИС;

– модуль метода экспертных оценок;

– модуль метода оценки защищенности информации от НСД;

– модуль формирования рекомендаций;

– модуль формирования отчета;

– документ отчетов.

Интерфейс программного комплекса обеспечивает взаимодействие пользователя с программным комплексом «Оценка защищенности информационной системы». Данный интерфейс упрощает взаимодействие по средствам интуитивного понятного расположения кнопок и окон ввода и вывода данных.

Модуль управления обеспечивает синхронизированную работу всех модулей, распределяет потоки данных, которые генерируются смежными модулями и поступают от пользователя.

Модуль подключения к информационной системе позволяет осуществить подключение ко всем компонентам ИС с помощью ввода аутентификационной информации и IP-адреса каждого компонента. Подключение может осуществляться с помощью двух типов подключения: SSH, TELNET.

Модуль сбора исходных данных обеспечивает сбор исходных данных из журналов со-

Архитектура программного комплекса

бытий ИС по каждому компоненту ИС. В данном модуле осуществляется их классификация, кроме того данный модуль реализует анализ угроз.

Модуль оценки защищенности ИС позволяет рассчитать количественную оценку защищенности ИС на основе данных полученных от модуля сбора данных.

Модуль метода экспертных оценок позволяет рассчитать количественную оценку данного метода. Для каждой актуальной угрозы производится расчет возможных реализаций угрозы, далее по каждому компоненту ИС производится расчет суммы рисков реализации угроз. По результатам проведенных расчетов высчитывается суммарная оценка защищенности ИС, на основе которой и определяется качественные оценки защищенности ИС.

Модуль метода оценки защищенности информации от НСД позволяет рассчитать количественную оценку данного метода. Модуль формирования рекомендаций реализует генерацию рекомендации по повышению уровня защищенности ИС на основе имеющихся сведений о состоянии защищенности ИС предприятия.

Модуль формирования отчета позволяет пользователю сохранять результаты работы программного комплекса, что в дальнейшем может служить пользователю основой для проведения сравнительного анализа изменения защищенности ИС в зависимости от применяемых мер по защите информации, кроме того данные отчеты могу быть применены при прогнозировании реализации угроз безопасности при использовании многокритериальных методов экстраполяции.

Документ отчетов позволяет хранить сформированные отчеты оценки защищенности ИС, в формате .docx.

Результат экспериментальных исследований показал повышение защищенности ИС при применении рекомендаций, генерируемых разработанным программным комплексом. В ходе экспериментального исследования подтверждена корректность работы программного комплекса.

СПИСОК ЛИТЕРАТУРЫ

1. Аветисян, А. И. Технологии статического и динамического анализа уязвимостей программного обеспечения / А. И. Аветисян, А. А. Белевацев, И. И. Чукляев // Вопросы кибербезопасности. – 2014. – № 3 (4). – С. 20–28.

2. Щеглов, К. А. Моделирование угроз атак на защищенную информационную систему / К. А. Щеглов, А. Ю. Щеглов // Известия высших учебных заведений. Приборостроение. – 2016. – Т. 59, № 12. – С. 980–990.

3. ISO/IEC 27004 – Информационная технология. Средства обеспечения безопасности. Измерения. – Электрон. текстовые дан. – Режим доступа: http://docs.cntd.ru/document/1200088532.

REFERENCES

1. Avetisyan A.I., Belevantsev A.A., Chuklyayev I.I. Tekhnologii staticheskogo i dinamicheskogo analiza uyazvimostey programmnogo

obespecheniya [Technologies for Static and Dynamic Analysis of Software Vulnerabilities]. *Voprosy kiberbezopasnosti*, 2014, no. 3 (4), pp. 20-28.

2. Shcheglov K.A., Shcheglov A.Yu. Modelirovaniye ugroz atak na zashchishchennuyu informatsionnuyu sistemu [Modeling of Threats of Attacks on a Secure Information System]. *Izvestiya vysshikh uchebnykh zavedeniy. Priborostroyeniye*, 2016, vol. 59, no. 12, pp. 980-990.

3. *ISO/IEC 27004 – Informatsionnaya tekhnologiya. Sredstva obespecheniya bezopasnosti. Izmereniya* [Information Technology. Security Tools. Measurements]. URL: http://docs.cntd.ru/document/1200088532.

METHODS OF DEVELOPING RECOMMENDATIONS FOR IMPROVING THE SECURITY OF INFORMATION SYSTEMS

Natalia A. Golovacheva

Senior Lecturer, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. With the advent of information technologies, information systems have been widely used in organizations and enterprises. The use of information systems allows optimizing the workforce, automating all or part of business processes. However, the use of information systems requires the development of an information security system to minimize malicious attacks. To reduce the likelihood of malicious attacks, there are a large number of software and hardware-based information security tools. The complexity of computing the distribution of the components of information systems complicates the process of creating and configuring protection systems, the number of threats to security are increasing every year. For a timely response to information security incidents, including attacks, it is necessary to use information system security assessment tools to reduce the risks of security breaches. InfoWath statistics show the growth trend of various types of attacks, both from an external attacker and from an internal one. Therefore, one of the most important tasks is to correctly determine the security of information systems. The paper implements a mathematical model for assessing the security of an information system based on the selected methods. The architecture of the software package for assessing the security of the information system is formed.

Key words: information security, mathematical model, expert assessment method, security assessment, security enhancement.

DOI: https://doi.org/10.15688/NBIT.jvolsu.2020.3.4

УДК 681.5:366.438
ББК 32.966

ЦИФРОВИЗАЦИЯ ПРЕДПРИЯТИЙ И ЭЛЕКТРОННАЯ ПАСПОРТИЗАЦИЯ ОБОРУДОВАНИЯ ОПАСНЫХ ПРОИЗВОДСТВЕННЫХ ОБЪЕКТОВ

Азиза Амануллаевна Кадырова

Кандидат технических наук,
заместитель директора Межотраслевого центра стратегических инноваций и информатизации
aziza.kaa@innovation.uz, aziza.kaa@mail.ru
ул. Университетская, 2, офис 214, 100095 г. Ташкент, Узбекистан

Аннотация. В статье рассматриваются и анализируются требования нормативных документов к эксплуатационной документации, порядок систематизации сведений по техническому устройств в течение всего периода его эксплуатации. Предложены принципы структурирования оборудования опасных производственных объектов.

Ключевые слова: цифровизация, техническое устройство, мониторинг, промышленная безопасность, эксплуатационная документация.

Стабильная безаварийная работа промышленных предприятий с опасными производственными объектами во многом зависит от надежной работы основного (технологического) оборудования, что обеспечивается проведением своевременных освидетельствований, технических обслуживаний и ремонтов в рамках автоматизированных систем управления техническим обслуживанием и ремонтами оборудования опасных производственных объектов (АСУ ТОиР ОПО). В этом плане электронная паспортизация оборудования или иначе создание электронных ремонтно-эксплуатационных паспортов (РЭП) является важнейшей составной частью работ по созданию АСУ ПБ.

Создание ремонтно-эксплуатационных паспортов оборудования обусловлено необходимостью цифровизации и охвата всего жизненного цикла работы оборудования: от установки до его списания. Ремонтно-эксплуатационный паспорт оборудования ОПО является источником информации по всем параметрам эксплуатации: технического облуживания, ремонтов, причин и продолжительности простоев, замен узлов и деталей, модернизации и передвижениях оборудования, финансовых затрат, аналитических выводов по различным срезам.

Остановимся на двух технологиях планирования ремонтов оборудования:

– первый из них, ремонт по техническому состоянию, базирующийся на информации о фактическом состоянии узлов и деталей оборудования. При этом контроль технического состояния выполняется с периодичностью и в объеме, установленными в нормативно-технической документации, а объем и момент начала ремонта определяется техническим состоянием изделия;

– вторая технология основана на учете наработок оборудования и его составных узлов (элементов). В этом случае остановка на ремонт осуществляется в соответствии с требованиями нормативно-технической документации.

Отметим, что в обоих случаях необходимо структурирование технологического оборудования на блоки, узлы, детали. Как правило, каждый узел, каждый элемент имеют свои номинальные ресурсы работы. Например, если оборудование состоит из сотен или нескольких тысяч элементов и узлов, то налицо наличие ровно такого же числа номинальных сроков службы. Для решения задачи автоматизированного учета наработки элементов и узлов оборудования необходимо в первую очередь воссоздать в памяти ЭВМ взаимосвязанную структуру узлов и деталей соответствующего технологического оборудования.

Отсюда ясно, что главные факторы сложности данного уровня производственных модулей – это прежде всего структурная сложность, недостаточное развитие методов математического моделирования технологического оборудования, отсутствие удобных с точки зрения использования ЭВМ моделей, позволяющих учитывать изменения в реальном масштабе времени наработок и остаточных ресурсов узлов и деталей и реализации автоматического мониторинга состояния оборудования, оптимального планирования и ремонтов оборудования [1–8].

Отмеченные выше обстоятельства подчеркивают особую актуальность исследований по созданию структурных методов моделирования, анализа и синтеза проектируемых и внедряемых в промышленности интегрированных автоматизированных систем управления и их взаимосвязанных внутриуровневых и межуровневых компонентов (систем).

В зависимости от целей моделирования могут быть синтезированы математические модели разных типов. В данной статье рассматриваются особенности построения теоретико-множественных графовых математических моделей, позволяющих воспроизвести в памяти компьютера оборудование и технологические сети (комплексы оборудования) ОПО как соответствующие иерархически упорядоченным взаимосвязанным множествам элементов с учетом изменения их эксплуатационных показателей во времени. Построенные в соответствии с этим принципом математические модели являются основой для решения на компьютере задач автоматизации процессов планирования и управления ремонтами, прогнозирования состояния оборудования на основе автоматического формирования динамически изменяющихся электронных баз данных (БД), учитывающих изменения эксплуатационных показателей.

Структурирование технологического оборудования ОПО

Воссоздание в памяти компьютера структуры оборудования, множеств взаимосвязанных узлов и деталей с соотнесенной к ним информацией о сроках службы (номинальных ресурсах), а также алгоритмов учета динамики простоев, наработок, остаточных ресурсов является необходимой основой для решения проблемы прогнозирования состояния оборудования, оптимизации планирования и управления ремонтами на базе разработанных информационного и программного обеспечений.

Принципы структурирования оборудования

В основу структурирования оборудования положены следующие основные принципы:

1. Оборудование для целей математического моделирования рассматривается с теоретико-множественных позиций.

2. Оборудование представляется в виде многоуровневой иерархической структуры.

3. Структурирование оборудования осуществляется до уровня далее неделимых элементов.

4. Каждому элементу (узлу) оборудования ставится в однозначное соответствие его идентификационный номер.

5. Помимо идентификационного номера каждый элемент (узел) оборудования имеет свои отличительные признаки, количественные или весовые характеристики, номинальный ресурс.

6. В качестве адекватной понятию «структура» и теоретико-множественной форме представления оборудования принимается ориентированный граф.

7. Структура технологической сети определяется как объединение множества графов единиц технологического оборудования.

С учетом вышеизложенного, можно предложить в качестве достаточно универсальной семиуровневую схему структуриро-

вания единиц технологического оборудования (см. рисунок).

Количество уровней 7:

– блок (1-й уровень);

– основное оборудование (2-й уровень);

– вспомогательное оборудование (3-й уровень);

– узлы (4-й уровень);

– узлы (5-й уровень);

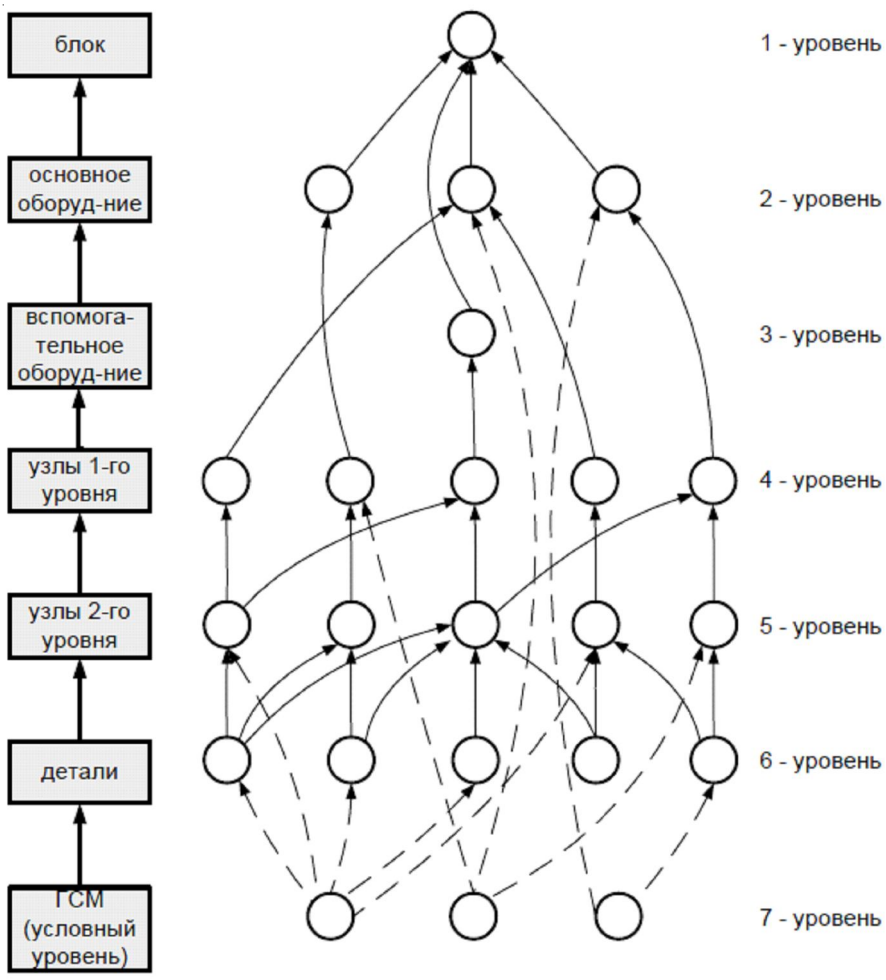
– детали (6-й уровень);

– условный 7-й уровень – ГСМ.

Стандартизация формы представления информации о технологическом оборудовании

Воссоздание в памяти ЭВМ структуры и состава технологического оборудования требует упорядочения информации в рамках стандартных таблиц, задающих однозначное соответствие между оборудованием, узлами, деталями и характеризующими их показателями. Возможная структура стандартизованной таблицы с учетом структурирования оборудования имеет вид (см. таблицу).

Паспорт технического устройства, безусловно, является основным эксплуатационным документом. В случае его утери (уничтожения) паспорт ТУ, его характеристические сведения должны быть обязательно восстановлены. Наличие основной эксплуатационной документации (паспортов, формуляров), сопровождающей техническое устройство в течение всего периода его эксплуатации, достоверность и грамотность ведения такой документации крайне важны для обеспечения продуктивного мониторинга технического состояния ТУ в течение всего назначенного срока службы, а возможно, и сверх такого срока. Мониторинг технического состояния оборудования, на опасных производственных объектах необходим не толь-



Макросхема многоуровневой схемы моделирования оборудования (*а*); граф-модель макросхемы (*б*)

Стандартизованная таблица оборудования

Наименование	Уровень сборки	Признак узла, детали (1 или 0)	Обозначение, тип, характеристики	Обозначение сборочного чертежа, ГОСТа	Материалы	Вес (кг)	Кол-во (шт.)	Срок службы	Дата установки	Дата замены	Всего заменено на дату запроса, причины замены	Способ установки
XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX

ко для контроля функционирования технических устройств в соответствии с их технологическим назначением, но и для поддержания необходимого уровня производственной безопасности на опасных производственных объектах.

СПИСОК ЛИТЕРАТУРЫ

1. Кадырова, А. А. Методы моделирования и исследования нелинейных и логико-динамических систем управления / А. А. Кадырова. – Ташкент : Янги аср авлоди, 2010. – 186 с.

2. Кадыров, А. А. Анализ методов математического моделирования дискретных динамических систем управления / А. А. Кадыров, А. А. Кадыров, А. А. Кадырова // Международная научно-практическая конференция «Инновация-2012» : сб. науч. ст. – Ташкент, 2012. – С. 223–226.

3. Кадыров, А. А. Декомпозиционные основы моделирования и исследования систем управления на базе динамических графов / А. А. Кадыров. – Ташкент : Иктисод-молия, 2015. – 226 с.

4. Кадыров, А. А. Динамические множества, графы и гиперграфы / А. А. Кадыров // Автоматическое управление. – Ташкент : Изд-во ТашПИ, 1979. – Вып. 273.

5. Кадыров, А. А. Теория разнотемповых дискретных систем управления / А. А. Кадыров. – Ташкент : Изд-во ТашГТУ, 2013. – 168 с.

6. Муромцев, Д. Ю. Анализ и синтез дискретных систем / Д. Ю. Муромцев, Е. Н. Яшин. – Тамбов : Изд-во ТГТУ, 2012. – 120 с.

7. Kadirov, A. A. Imitative Simulation of Structurally Complex System Based on Dynamic Graphs / A. A. Kadirov // System Analysis. – 1990. – № 5. – P. 35–43.

8. Kadirova, D. R. Complex Discrete Systems Graph Simulation / D. R. Kadirova, A. A. Kadirova // Journal of Multimedia and Information System. – 2015, Sep. – Vol. 2, № 3. – P. 263–274. – DOI: http://dx.doi.org/ 10.9717/JMIS.2015.2.3.263.

REFERENCES

1. Kadyrova A.A. *Metody modelirovaniya i issledovaniya nelineynykh i logiko-dinamicheskikh sistem upravleniya* [Methods of Modeling and Research of Non-Linear and Logical-Dynamic Control Systems]. Tashkent, Yangi asr avlodi Publ., 2010. 186 p.

2. Kadyrov A.A., Kadyrov A.A., Kadyrova A.A. Analiz metodov matematicheskogo modelirovaniya diskretnykh dinamicheskikh system upravleniya [Analysis of Methods of Mathematical Modeling of Discrete Dynamic Control Systems]. *Mezhdunarodnaya nauchno-prakticheskaya konferentsiya «Innovatsiya-2012»: sb. nauch. st.* [Proceedings of International Scientific and Practical Conference Innovation-2012]. Tashkent, 2012, pp. 223-226.

3. Kadyrov A.A. *Dekompozitsionnye osnovy modelirovaniya i issledovaniya sistem upravleniya na baze dinamicheskikh grafov* [Decomposition Bases for Modeling and Research of Control Systems Based on Dynamic Graphs]. Tashkent, Iktisod-moliya Publ., 2015. 226 p.

4. Kadyrov A.A. Dinamicheskie mnozhestva, grafy i gipergrafy [Dynamic Sets, Graphs, and Hypergraph s]. *Avtomaticheskoe upravlenie* [Automatic Control]. Tashkent, TashPI Publ., 1979, iss. 273.

5. Kadyrov A.A. *Teoriya raznotempovykh diskretnykh sistem upravleniya* [The Theory of Multiple-Time-Scale Discrete Control Systems]. Tashkent, TashGTU Publ., 2013. 168 p.

6. Muromtsev D.Yu., Yashin E.N. *Analiz i sintez diskretnykh sistem* [Analysis and Synthesis of Discrete Systems]. Tambov, TGTU Publ., 2012. 120 p.

7. Kadirov A.A. Imitative Simulation of Structurally Complex System Based on Dynamic Graphs. *System Analysis*, 1990, no. 5, pp. 35-43.

8. Kadirova D.R., Kadirova A.A. Complex Discrete Systems Graph Simulation. *Journal of Multimedia and Information System*, 2015, vol. 2, no. 3, pp. 263-274. DOI: http://dx.doi.org/10.9717/JMIS.2015.2.3.263.

DIGITALIZATION OF ENTERPRISES AND ELECTRONIC CERTIFICATION OF EQUIPMENT OF HAZARDOUS PRODUCTION FACILITIES

Aziza A. Kadyrova

Candidate of Sciences (Engineering),
Deputy Director of Center for Strategic Innovations and Informatization
aziza.kaa@innovation.uz, aziza.kaa@mail.ru
Universitetskaya St, 2, office 214, 100095 Tashkent, Uzbekistan

Abstract. Stable trouble-free operation of industrial enterprises with hazardous production facilities largely depends on the reliable operation of the main (technological) equipment, which is ensured by timely inspections, technical services and repairs within automated control systems for the maintenance and repair of equipment of hazardous production facilities. In this regard, the electronic certification of equipment or otherwise the creation of electronic repair and maintenance passports is the most important part of the work on the creation of a digital enterprise. The creation of repair and maintenance certificates of equipment is due to the need for digitalization and coverage of the entire life cycle of the equipment: from installation to its decommissioning. The repair and operational passport of equipment of hazardous production facilities is a source of information on all parameters of operation: technical maintenance, repairs, causes and duration of downtime, replacement of components and parts, modernization and movement of equipment, financial costs, analytical conclusions on various cross-sections. The article discusses and analyzes the requirements of regulatory documents for operational documentation, the order of systematization of information on technical equipment during the entire period of its operation. The principles of structuring the equipment of hazardous production facilities are proposed.

Key words: digitalization, technical device, monitoring, industrial safety, operational documentation.

DOI: https://doi.org/10.15688/NBIT.jvolsu.2020.3.5
УДК 004.77:005.334
ББК 32.971.35

АНАЛИЗ УГРОЗ И УЯЗВИМОСТЕЙ КОНЦЕПЦИЙ IoT И IIoT

Вадим Юрьевич Шевцов

Ассистент кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Никита Павлович Касимовский

Студент кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. данная статья описывает концепции IoT и IIoT угрозы информационной безопасности для них. Рассмотрены концепции интернета вещей и промышленного интернета, виды возможных устройств, основные проблемы информационной безопасности. Также выделены рекомендации по защите данных технологий и приведены результаты исследований крупных компаний в данной области.

Ключевые слова: интернет вещей, промышленный интернет, ботнет, кибербезопасность, вредоносное ПО.

IoT (интернет вещей) – система взаимосвязанных компьютерных сетей и подключенных физических объектов (вещей) со встроенными сенсорами и программным обеспечением для манипуляции с данными, с возможностью удаленного контроля и управления в автоматизированном режиме, без участия пользователя [2; 5].

IoT включает в себя несвязанные между собою разрозненных сетей, каждая из которых была построена для решения конкретных задач. Как пример можно привести работу современных автомобилей, в которых функционирует сразу несколько различных сетей: первая отвечает за функционирование двигателя, вторая управляет системами безопасности, третья поддерживает связь и т. д. В различных зданиях устанавливаются аналогичные сети для управления коммунальными системами, средствами безопасности и прочие. По мере развития Интернета вещей множественные сети будут объединяться и получать большие возможности в области безопасности, аналитики и управления. В итоге IoT предлагает человечеству более широкие перспективы для реализации его потенциала (см. рис. 1).

Технологии Интернета вещей:

– подключение:

– 2G/3G/4G, 5G Спутниковая (VSAT), LPWAN (LORA, LTE-M, NB IOT, NB FI и т. д.), сетевые подключения;

– оборудование:

– датчики;

– аппаратные модули защиты информации;

– серверы;

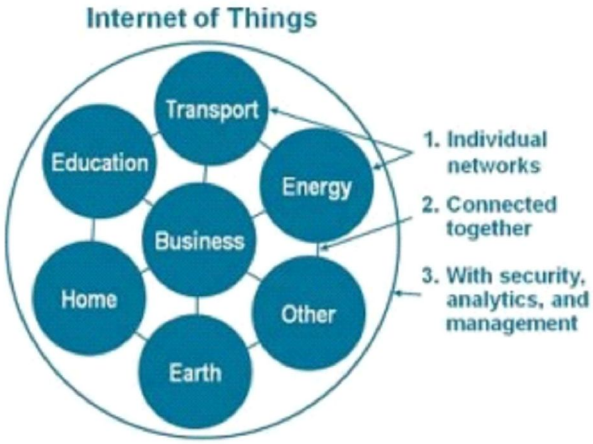


Рис. 1. Возможная схема взаимодействия различных сфер жизнедеятельности с использованием технологий интернета вещей

– СХД;
– иные устройства (специальное оборудование);
– услуги:
– системы по управлению компонентами ИВ;
– аутсорсинг инфраструктуры;
– хостинг и управление приложениями;
– информационные услуги (системная интеграция, разработка приложений) и ввод устройств;
– программное обеспечение:
– программы аналитики;
– прикладные приложения;
– кросс-индустриальные платформы;
– индустриальные платформы;
– программное обеспечение защиты информации;
– другое программное обеспечение.

Экспертное сообщество утверждает, что производители услуг и оборудования сферы IoT не выполняют принцип сквозной информационной безопасности, необходимый для информационных технологий. Исходя из этого информационная безопасность должна закладываться на исходном этапе проектирования устройства или услуги и поддерживаться вплоть до завершения их жизненного цикла.

К примеру, часть данных наблюдений компании HP (лето 2014 г.), целью которых являлось не обнаружить определенные уязвимые интернет-устройства и уличить их производителей, но актуализировать тему ИБ-рисков в сфере IoT в целом.

Эксперты HPE делают акцент на проблемах, как со стороны пользователей устройств, так и на проблемы, уделить внимание которым должны производители. Изначально пользователю необходимо произвести настройку пароля, сменив пароль разработчика, используемый по умолчанию, на стойкий, так как пароли разработчика одни и те же на разных устройствах и имеют низкую надежность. Однако далеко не каждый следует этому правилу. Поскольку не каждое устройство содержит встроенный функционал ИБ, пользователям рекомендуется произвести установку дополнительной защиты, предназначенной для личного пользования, для того чтобы интернет-устройства не превратились в открытую дверь внутренней сети или непосредственной причиной нанесения ущерба.

В результате исследования HP обнаружено, что около 70 % выбранных устройств не использует шифрование в беспроводной передаче данных. Веб-интерфейс 60 % устройств исследователи HP признали уязвимым из-за небезопасной реализации доступа и большого риска межсайтового скриптинга. Во многих устройствах используются пароли невысокой надежности. Около 90 % устройств используют телеметрию, собранную о владельце без его согласия.

Также исследователи HP выявили около 25 всевозможных уязвимостей в каждом из выбранных устройств (телевизоров, дверных замков, бытовых весов, домашних охранных систем, электророзеток и т. п.) и в их веб-компонентах.

Вывод исследователей HP настораживает: безопасная система IoT на данный момент отсутствует. Основную опасность IoT представляют в предмете распространения целевых атак. Как только злоумышленники решат воздействовать на кого-либо, и наши верные помощники из мира IoT превращаются в предателей, нараспашку открывающих доступ в мир своих владельцев.

Уязвимые места интернета вещей:

– IPv6;

– питание сенсоров;

– стандартизация архитектуры и протоколов, сертификация устройств;

– обеспечение защиты информации;

– учетные записи по умолчанию, низкая надежность механизмов аутентификации;

– отсутствие сопровождения продуктов от производителя для решения проблем безопасности;

– невозможность обновить программно-аппаратной составляющей;

– использование открытых протоколов и лишних открытых портов;

– зависимость безопасности сети от конкретных устройств;

– использование слабозащищенных мобильных технологий

– использование незащищенной облачной инфраструктуры;

– использование уязвимого программного обеспечения

Как вариант, не исключается установка на устройства сети специальных уникальных чипов, которые обезопасят их от атак хакеров. Такие меры должны увеличить уровень доверия к IoT в обществе и помешать злоумышленникам реализовывать ботнеты из подключаемой техники (см. таблицу).

В первой половине 2019 г. специалисты из «Лаборатории Касперского» с помощью приманок для злоумышленников зафиксировали 105 млн атак на IoT-устройства, исходящих с 276 тыс. уникальных IP-адресов. Данный показатель в семь раз больше, чем в первой половине 2018 г., когда было обнаружено около 12 млн атак с 69 тыс. IP-адресов. Пользуясь практически отсутствующей защитой IoT-продуктов, злоумышленники прикладывают больше усилий для создания и монетизации IoT-ботнетов.

Количество атак на IoT-устройства постоянно растет, потому что пользователи и организации все чаще приобретают «умные» устройства, такие как роутеры или камеры видеонаблюдения, но при этом мало кто заботится об их защите и установке актуальных обновлений. Злоумышленники, в свою очередь, видят все больше финансовой выгоды в эксплуатировании таких устройств. Они используют сети зараженных «умных» устройств для проведения DDoS-атак или в качестве прокси-сервера для других типов вредоносных действий.

Согласно полученным данным, атаки на IoT-устройства не выделяются сложной реализацией, но являются достаточно незаметными для рядовых пользователей. Самым популярным типом вредоносных программ, который позволяет ботнетам компрометировать устройства с помощью старых уязвимостей и управлять ими, является Mirai. Данное семейство программного обеспечения применялось в 39 % от всех атак. Второе место занимает вредоносное ПО Nyadrop (38,57 %), которое использует брут-форс в своей реализации, а также часто использовался в качестве загрузчика Mirai. Третьим наиболее рас-

Статистика и прогноз расходов на сервисы безопасности [4]

	2016	2017	2018	2019	2020	2021
Endpoint Security	240	302	373	459	541	631
Gateway Security	102	138	186	251	327	415
Professional Services	570	734	946	1,221	1,589	2,071
Total	**912**	**1,174**	**1,506**	**1,931**	**2,457**	**3,118**

пространенным ботнетом стал Gafgyt (2,12 % от всех атак) (рис. 2) [3].

Исследователи также определили страны, которые чаще других оказывались источниками атак в первом полугодии 2019 года. 30 % от общего числа атак исходило из Китая, из Бразилии – 19 %, далее Египет с долей в 12 %. В первом полугодии 2018 г. положение оказалось другим – Бразилия являлась первой с долей 28 %, Китай был источником 14 % атак, а третьей оказалась Япония с 11 % [3].

Внутри IoT-систем накопление информации происходит в режиме реального времени. К примеру, информация о занятости индустриальных систем, информация необходимая для управления дорожным трафиком, информация о текущем состоянии человека, видео, текстовая информация и т. д. Устройства, отправляющие такую информацию, могут оказаться уязвимыми, из-за чего возможна утечка важных данных. К тому же небезопасными могут оказаться протоколы взаимодействия составных частей интернета вещей. Это обстоятельство имеет высокую актуальность. Если в прошлом устройства зачастую использовали клиент-серверную модель и представляли собой частные сети, то сейчас многие устройства подключаются друг к другу напрямую, при этом в этом случае облачная платформа используется для управления и сбора статистики. Это размывает границы информационной безопасности и заставляет организации пересматривать подходы к организации защиты на сетевом уровне.

Рассматривая прикладные протоколы с позиции производителей, получается огромный арсенал механизмов взаимодействия, стандарты не регулируются. Есть только несколько стандартных прикладных протоколов, например MQTT, CoAP и AMQP. Но большинство производителей IoT-устройств изначально производили электрооборудование, и когда они реализуют собственные протоколы и стандарты, то нечасто задумываются о безопасности.

Иная угроза – это возможность взлома локальных устройств в целях проведения вредоносного воздействия на инфраструктуру предприятия или путем использования IoT. Например одна из версий вредоносной сети Mirai внедрилась в более 5 миллионов устройств, считая и IoT в 164 странах мира. В результате у интернет-провайдера в Германии была заражена большая часть роутеров, что привело к серьезным репутационным и материальным потерям.

Другая угроза – это несанкционирование завладение правами администратора в устройствах IoT и изменение исходящих пакетов. К примеру, если IoT применяется в здравоохранении, то доктор получит некорректную информацию о самочувствии больного (от сенсора) и пропишет неправильное лечение.

Реализация безопасности конечных устройств при установке IoT содержит следующие этапы:

– анализ патча программно-аппаратной системы с последующей сертификацией на

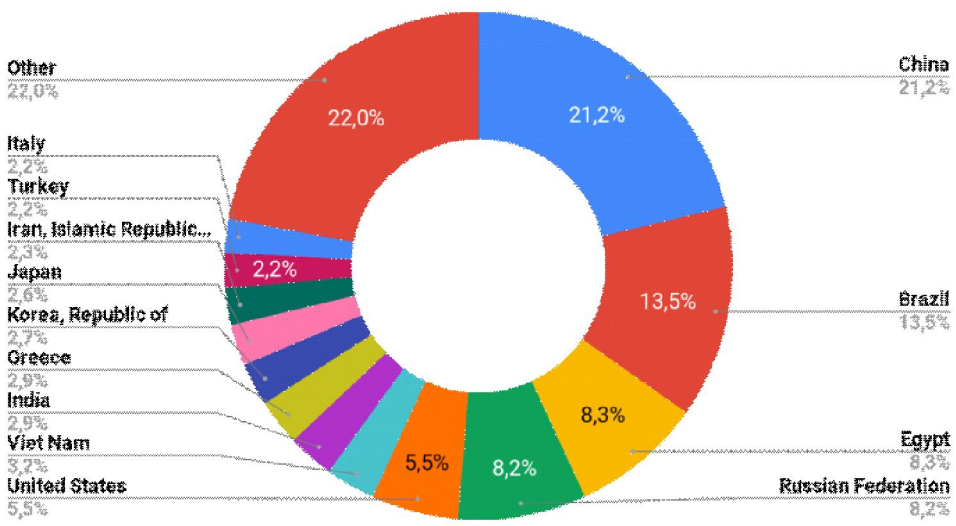


Рис. 2. Страны – источники атак на ханипоты за 2018 г.

отсутствие возможностей не указанных в документации;

– повышение безопасности встроенной операционной системы;

– обнаружение уязвимостей в непосредственной работе;

– правильное конфигурирование брандмауэра по умолчанию, предотвращение вторжений на прикладном уровне и на уровне протоколов передачи данных;

– использование технологий виртуальных частных сетей;

– проверка неизменности прошивки

– реализация общего механизма сертификации либо децентрализованной доверенной системы аутентификации для обеспечения связи между различными устройствами.

К тому же необходимо защитить облачные вычислительные мощности, осуществляющую управление и мониторинг, агрегацию и анализ информации, получаемой от устройств интернета вещей. Затем следует выборать брандмауэр, WAF, систему обнаружения и предотвращения атак, VPN, реализовать систему противодействия DDoS и отслеживанию действий клиентов, SIEM. Для всех систем необходимо выработать специальные требования в целях обеспечения безопасности устройств интернета вещей.

IIoT – многоуровневая система, имеющая в своем составе контроллеры и датчики, размещенные на узлах и агрегатах индустриальной системы, система передачи получаемой информации и ее отображения, инструменты аналитики и интерпретации получаемых данных и другие компоненты (рис. 3) [2].

Технология имеет следующую особенность: сначала вводятся сенсоры, механизмы исполнения, контроллеры и HMI в базовых элементах оборудования, затем производится получение данных, в дальнейшем позволяющих предприятию получить реальную информацию о текущем положении систем. Обработанные данные поступают в каждый департамент организации, в результате чего совместная работа сотрудников разных отделов становится быстрее и выносятся обоснованные решения.

Также организациям становится доступна замена традиционного документооборота.

Собираемые данные возможно применить в целях недопущения приостановки работ, неисправностей оборудования, снижения риска проведения экстренного техобслуживания и проблем проведении цепочек поставок, что дает возможность предприятию значительно повысить производительность труда.

В процессе структурирования необработанных больших массивов данных и фильтрации, объективная интерпретация является основной задачей для организаций. Здесь первостепенным значением становится корректное представление информации в понятном пользователю виде, для этого сегодня на рынке представлены прогрессивные аналитические платформы, предназначенные для сбора, хранения и анализа данных о технологических процессах и событиях в реальном времени.

Рис. 3. Сферы применения технологий IIoT [1]

Благодаря этим решениям производственные данные преобразуются в полезную информацию, необходимую для безопасного и рационального управления предприятием.

Внедрение таких технологий дает возможность предприятиям из разных отраслей экономики получить определенные преимущества:

– увеличить эффективность использования производственных активов на 10 % за счет сокращения количества незапланированных простоев;

– снизить затраты на техническое обслуживание на 10 %, усовершенствовав процедуры прогнозирования и предотвращения катастрофических отказов оборудования и выявляя неэффективные операции;

– повысить производительность на 10 %, увеличить уровень энергоэффективности и сократить эксплуатационные расходы на 10 % за счет более эффективного использования энергии.

Таким образом, передовые технологии позволяют предприятиям из различных отраслей промышленности добиться существенных конкурентных преимуществ.

11 февраля 2019 г. появилась информация о том, что Международная организация по стандартизации (ИСО/ISO) разработала стандарт ISO/TR 22100-4:2018 «Безопасность производственного оборудования – Связь с ISO 12100 – Часть 4: Руководство для производителей оборудования по рассмотрению соответствующих аспектов информационной безопасности (ISO/TR 22100-4:2018 Safety of machinery – Relationship with ISO 12100 – Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects). Документ был опубликован в декабре 2018 года [6].

Глубокое проникновение промышленного интернета вещей в критически важную инфраструктуру и производственный сектор приводит к увеличению числа атак на информационные структуры предприятий. Об этом свидетельствуют данные исследования, проведенного аналитиками компании Frost & Sullivan, о чем стало известно 13 декабря 2018 года.

Согласно мнению экспертов, атаки только на энергетические и коммунальные отрасли обходятся предприятиям в среднем в $13,2 млн ежегодно. Специалисты Frost & Sullivan выделяют, что увеличение рисков является одной из причин разработки общих подходов к обеспечению информационной безопасности.

В отчете Frost & Sullivan указано несколько рекомендаций для развития компаний на рынке услуг обеспечения кибербезопасности. Одной из таких рекомендаций является создание интегрированных платформ, реализующих требуемый показатель защищенности конечных пользователей, одновременное внедрение лучших практик обеспечения ИБ, использование автоматизированных сервисов управления и расширенной аналитики для разработки комплексного портфеля услуг, который может быть адаптирован для всех типов конечных пользователей. Кроме того, аналитики считают перспективными гибкие модели ценообразования и подход CSaaS (Cybersecurity-as-a-Service – «кибербезопасность как услуга»).

Согласно результатам исследования «Лаборатории Касперского», инциденты с устройствами интернета вещей входят в тройку угроз с наибольшим финансовым ущербом для компаний. Это относится к компаниям любого размера: от малого бизнеса до больших корпораций.

По информации «Лаборатории Касперского», одной из главных проблем в сфере кибербезопасности индустриальных IoT-устройств является отсутствие единых стандартов. Рекомендации ENISA, как ожидается, станут важным шагом в сторону единообразия практик и политик безопасности, причем они касаются как создателей и пользователей промышленных IoT-устройств, так и разнообразных агентств Евросоюза, разрабатывающих политики безопасности.

Среди основных рекомендаций, разработанных для регуляторов:

– фокус на конкретных рекомендациях вместо общих для каждого сектора;

– стандартизировать рекомендации внутри ЕС, установить единую терминологию и классификацию;

– сотрудничать с представителями индустрии и вовлекать частный сектор в разработку законов, используя действующие ассоциации и объединения, например, AIOTI.

Главные рекомендации для производителей устройств и разработчиков ПО:

– убедиться, что с сотрудниками проведены беседы в области кибербезопасности, и

они обучены навыкам в области защиты информации;

– обеспечить совместимость данных с доверенной автоматизированной системой установки обновлений;

– провести проверку кода во время процесса установки – это уменьшит количество ошибок в конечной версии продукта, а также выявит любые попытки злоумышленника внедрить вредоносное программное обеспечение или обойти аутентификацию.

Популярность промышленного интернета вещей планомерно растет вместе с развитием интернета вещей. Оба этих подхода предполагают обмен данными через интернет, используют общие аппаратные платформы и управляются при помощи специализированного программного обеспечения, и это приводит к тому, что увеличивается количество общих уязвимостей и возможных атак на объекты промышленного сектора. Из отчета Frost & Sullivan следует, что промышленная и IT-инфраструктуры становятся прозрачнее. В первую очередь это связано с развитием стандарта Industrial 4.0 и отказ от изолирования промышленных объектов, что влечет за собой общие уязвимости, использование сервисов безопасности по модели SaaS для объектов промышленности, а также использование аппаратных устройств, доступ к которым потенциальный злоумышленник может получить довольно легко.

Если говорить про подход к защите IoT-систем в целом, то это нужно делать параллельно с определением требований информационной безопасности, то есть проводить подробный анализ рисков, которые появляются с внедрением различных технологий интернета вещей, и выстраивать систему с учетом максимально возможного уменьшения этих рисков. В текущей ситуации рекомендуется применять интернет вещей только для тех бизнес-процессов, для которых нарушение работоспособности не приводит к плачевным последствиям для бизнеса и здоровья людей.

СПИСОК ЛИТЕРАТУРЫ

1. Будущее за промышленным интернетом: телеком-компании нашли ниши для роста. – Электрон. текстовые дан. – Режим доступа: https://yamobi.ru/posts/iiot-2016.

2. Зачем вам нужен Splunk? Интернет вещей и промышленные данные. – Электрон. текстовые дан. – Режим доступа: https://www.securitylab.ru/blog/company/ts-solution/344595.php.

3. Интернет вещей (IoT): история зловредов. – Электрон. текстовые дан. – Режим доступа: https://securelist.ru/iot-a-malware-story/94900/

4. Информационная безопасность интернета вещей (Internet of Things). – Электрон. текстовые дан. – Режим доступа: https://www.tadviser.ru/index.php/%D1%F2%E0%F2%FC%FF:%C8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%ED%E0%FF_%E1%E5%E7%EE%EF%E0%F1%ED%EE%F1%F2%FC_%E8%ED%F2%E5%F0%ED%E5%F2%E0_%E2%E5%F9%E5%E9_%28Internet_of_Things%29

5. Технологическая платформа интернета вещей: стандарты, возможности, перспективы. – Электрон. текстовые дан. – Режим доступа: https://www.tssonline.ru/articles/tekhnologicheskaya-platforma-interneta-veshchej-standarty-vozmozhnosti-perspektivy.

6. ISO/TR 22100-4:2018 Safety of machinery – Relationship with ISO 12100. – Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects.

REFERENCES

1. *Budushchee za promyshlennym internetom: telekom-kompanii nashli nishi dlya rosta* [The Future of the Industrial Internet: Telecom Companies Have Found Niches for Growth]. URL: https://yamobi.ru/posts/iiot-2016.

2. *Zachem vam nuzhen Splunk? Internet veshchej i promyshlennye dannye* [Why do you Need to Splunk? Internet of Things and Industrial Data]. URL: https://www.securitylab.ru/blog/company/ts-solution/344595.php.

3. *Internet veshchej (IoT): istoriya zlovredov* [Internet of Things (IoT): A History of Malware]. URL: https://securelist.ru/iot-a-malware-story/94900.

4. *Informacionnaya bezopasnost' interneta veshchej (Internet of Things)* [Information Security of the Internet of Things (Internet of Things)]. URL: https://www.tadviser.ru/index.php/%D1%F2%E0%F2%FC%FF:%C8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%ED%E0%FF_%E1%E5%E7%EE%EF%E0%F1%ED%EE%F1%F2%FC_%E8%ED%F2%E5%F0%ED%E5%F2%E0_%E2%E5%F9%E5%E9_%28Inter net_of_Things%29.

5. *Tekhnologicheskaya platforma interneta veshchej: standarty, vozmozhnosti, perspektivy* [The Technological Platform of the Internet of Things:

Standards, Opportunities, Prospects]. URL: https://www.tssonline.ru/articles/tekhnologicheskaya-platforma-interneta-veshchej-standarty-vozmozhnosti-perspektivy.

6. *ISO/TR 22100-4:2018 Safety of machinery – Relationship with ISO 12100. Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects*.

THREAT AND VULNERABILITY ANALYSIS OF IoT AND IIoT CONCEPTS

Vadim Yu. Shevtsov

Assistant Lecturer, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Nikita P. Kasimovsky

Student, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. IoT and IIoT are new information technologies. They are very efficient solutions for home, industry and infrastructure. A lot of complex processes can be implemented using this systems. The popularity of the industrial Internet of things is steadily growing along with the development of the Internet of things. Both of these approaches involve the exchange of data over the Internet, use of common hardware platforms and are managed by using specialized software, and this leads to an increase in the number of common vulnerabilities and possible attacks on industrial facilities. The Frost & Sullivan report shows that industrial and IT infrastructures are becoming more transparent. First of all, this is due to the development of the Industrial 4.0 standard and the refusal to isolate industrial facilities, which entails common vulnerabilities, the use of security services based on the SaaS model for industrial facilities, as well as the use of hardware devices that a potential attacker can access quite easily. But very actual problems of IoT and IIoT are information security. Many of this systems are critical and little error can stop the entire system. This is not hard for hackers because that complex system has sensitive components usually. For example simple router can have a lot of vulnerabilities. There an attacker takes a root easily in every system. To solve the problem successfully it is recommended to use complex security actions. These are secure configurations of network devices, using safe devices and protocols, regular audit, using backups, using actual politics of information security.

Key words: IoT, IIoT, botnet, cybersecurity, malicious software.

www.volsu.ru

ИННОВАЦИИ В МЕТАЛЛУРГИИ
И МАТЕРИАЛОВЕДЕНИИ

DOI: https://doi.org/10.15688/NBIT.jvolsu.2020.3.6

УДК 539.2:669.155.3
ББК 34.2

ИССЛЕДОВАНИЕ ТОНКОЙ СТРУКТУРЫ ОБРАЗЦОВ ИЗ НИОБИЕВОГО СПЛАВА 5 ВМЦ ПОСЛЕ ВНУТРЕННЕГО АЗОТИРОВАНИЯ

Константин Олегович Смирнов

Старший преподаватель кафедры судебной экспертизы и физического материаловедения,
Волгоградский государственный университет
priori@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В работе рассматривается возможность изучения тонкой структуры образцов из ниобиевого сплава 5 ВМЦ (марка 5В2МЦ-2), прошедших внутреннее азотирование методом рентгеноструктурного анализа. Показан расчет плотности дислокаций, представляющий один из параметров тонкой структуры с помощью различных методик. Рассмотрено его влияние на возможные режимы внутреннего азотирования.

Ключевые слова: рентгеноструктурный анализ, плотность дислокаций, упрочнение ниобиевых сплавов.

Введение

Создание перспективных конструкционных жаропрочных сплавов, обладающих достаточным запасом пластичности, является одной из важнейших инновационных задач материаловедения.

Известно, что ниобий по комплексу важнейших физико-химических, механических и технологических свойств является наиболее перспективным и ценным материалом для использования в атомной энергетике, ракетной и авиационной технике [5; 7].

Наиболее перспективным способом упрочнения ниобиевых сплавов является введение высокостабильных фаз внедрения нитридов, оксидов, карбидов, инертных относительно матрицы [2; 3].

В задачах практического использования азотированных сплавов принципиальным является вопрос о термической стабильности структуры. Так, упрочнение жаропроч-

ных ниобиевых сплавов может быть связано с использованием особенностей ультрамелкозернистой структуры с ультрадисперсными нитридами (реализация дислокационной ячеисто-нитридной структуры, в которой растворимость азота превышает равновесное значение). Выделение избыточной фазы при таком дисперсном упрочнении будет происходить не сразу, а в процессе дополнительных вакуумных отжигов, благодаря чему удается избежать охрупчивания металла из-за возникновения слоя поверхностных нитридов.

При деформации некоторых металлов и сплавов (в основном твердых растворов) может происходить принципиальная перестройка их тонкой структуры, связанная с образованием ячеек. Под параметрами тонкой структурой металла [6; 8] обычно понимают размер блоков (областей когерентного рассеяния рентгеновских лучей), уровень внутренних искажений в кристаллах и плотность линейных дефектов, таких как плотность дислокаций.

Известно, что азот является наиболее эффективным упрочнителем ниобиевых сплавов. Нитриды в качестве упрочняющей фазы в ниобии и некоторых других тугоплавких металлах обладают некоторыми преимуществами перед карбидами: они термодинамически более стабильные соединения, имеющие относительно узкие области гомогенности и низкий уровень растворимости. Эти качества нитридов позволяют вводить в сплавы большие объемные содержания упрочняющей фазы и сохранять ее дисперсность в процессе длительной службы сплава при высоких температурах [2].

Фазы внедрения (оксиды, карбиды, нитриды) способствуют повышению сопротивления ползучести и длительной прочности, являясь преградами на пути движения дислокаций, а также препятствуют рекристаллизации при высоких температурах, блокируя границы зерен.

При этом дисперсность выделяющихся нитридов не зависит от глубины внутреннего азотирования, а их размер имеет исключительно высокую дисперсность (радиус не превышает 4–10 нм). Термическая стабильность нитридов при этом может достигать 1 600 °С [2; 3].

Также благодаря стабилизирующему действию нитридов возможно повышение жаропрочности тугоплавких металлов. Образовавшееся покрытие при азотировании препятствует движению и выходу дислокаций на поверхность. При азотировании ниобиевых сплавов температура начала рекристаллизации может повышаться на 350 °С [2]. Жаропрочность может значительно повыситься с увеличением концентрации легирующих элементов. Таким образом зона внутреннего азотирования будет полностью определяться созданием диффузионного слоя, который будет определяться выбранным режимом химико-термической обработки [4].

Исследование образцов

Для исследования были выбраны образцы, изготовленные из ниобиевого сплавов 5 ВМЦ (марки 5В2МЦ-2 согласно ГОСТ 26468-85 Сплавы деформируемые на основе ниобия. Марки) со следующим химическим составом: мас. %: 4,5...5,6 W; 1,7...2,3 Mo; 0,7...1,15Zr; 0,02 C.

Данный сплав относится к низколегированным жаропрочным сплавам ниобия с твердорастворным упрочнением и обладает высокими показателями жаропрочности и низкотемпературной пластичности.

Исследуемые образцы прошли внутреннее азотирование по следующим режимам: образец № 1 550 °С – 10 ч + вакуумный отжиг 1200° – 1,5 ч; № 2 800 °С – 10 ч + вакуумный отжиг 1000° – 1,5 ч, 1200° – 1 ч, а также исходный образец № 3 – ниобиевый сплав 5 ВМЦ без азотирования.

Рентгеноструктурный анализ проводился на рентгеновском дифрактометре ДРОН-3М в медном и железном излучении (см. рис. 1–8).

По данным дифрактограмм, используя различные методики расчета [1; 3; 6], были получены значения плотности дислокаций.

Проведенный расчет показал, что полученные результаты имеют приблизительно равные значения в размерах степенного показателя (см. таблицу).

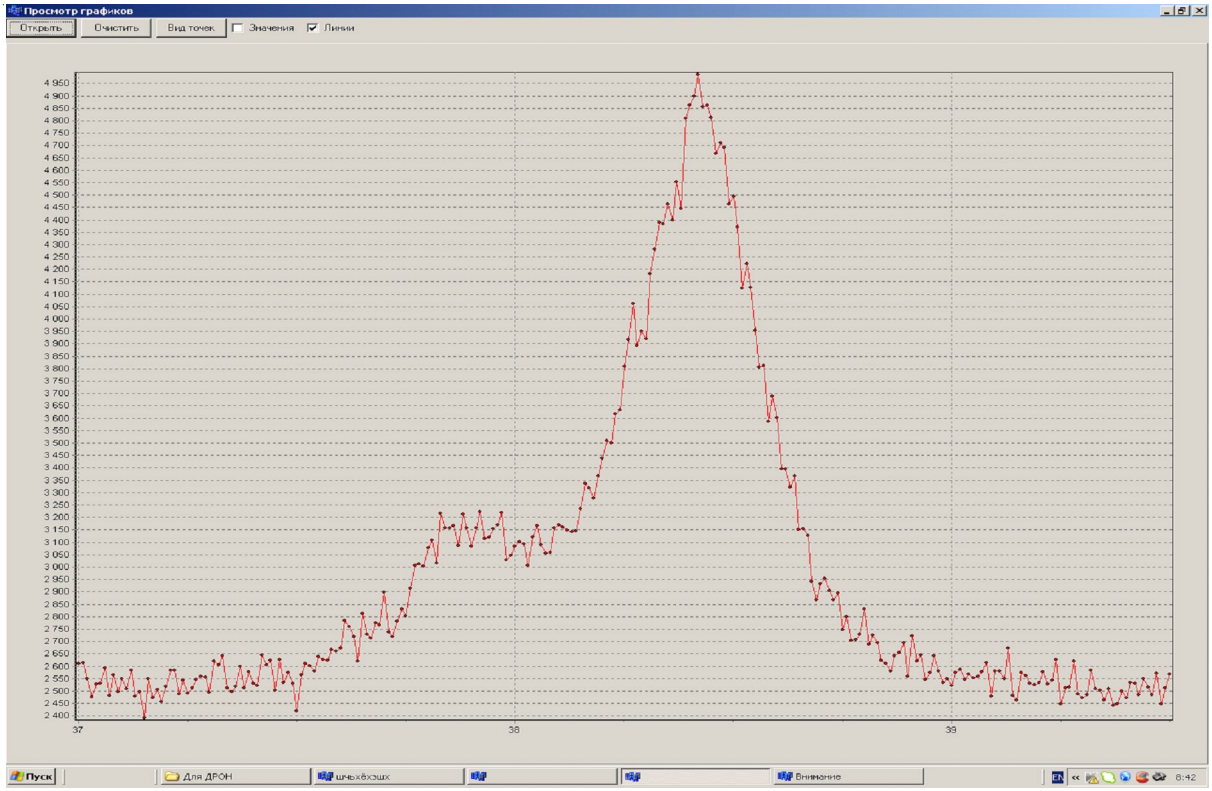


Рис. 1. Фрагмент дифрактограммы образца из ниобиевого сплава 5 ВМЦ, после азотирования 800 °С – 10 ч и отжигов 1,5 ч – 1000 °С и 1 ч – 1200 °С. Линия $(110)_{\alpha}$

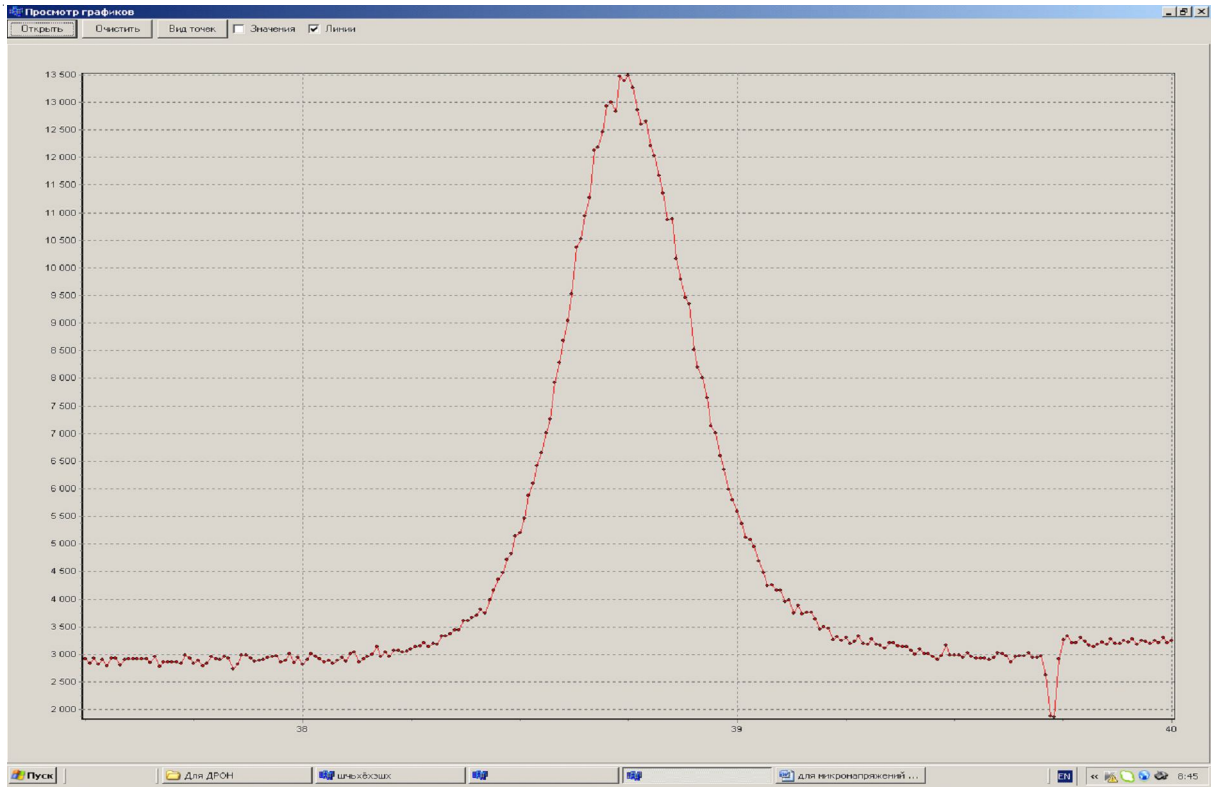


Рис. 2. Фрагмент дифрактограммы образца из ниобиевого сплава 5 ВМЦ в исходном состоянии. Линия $(110)_{\alpha}$

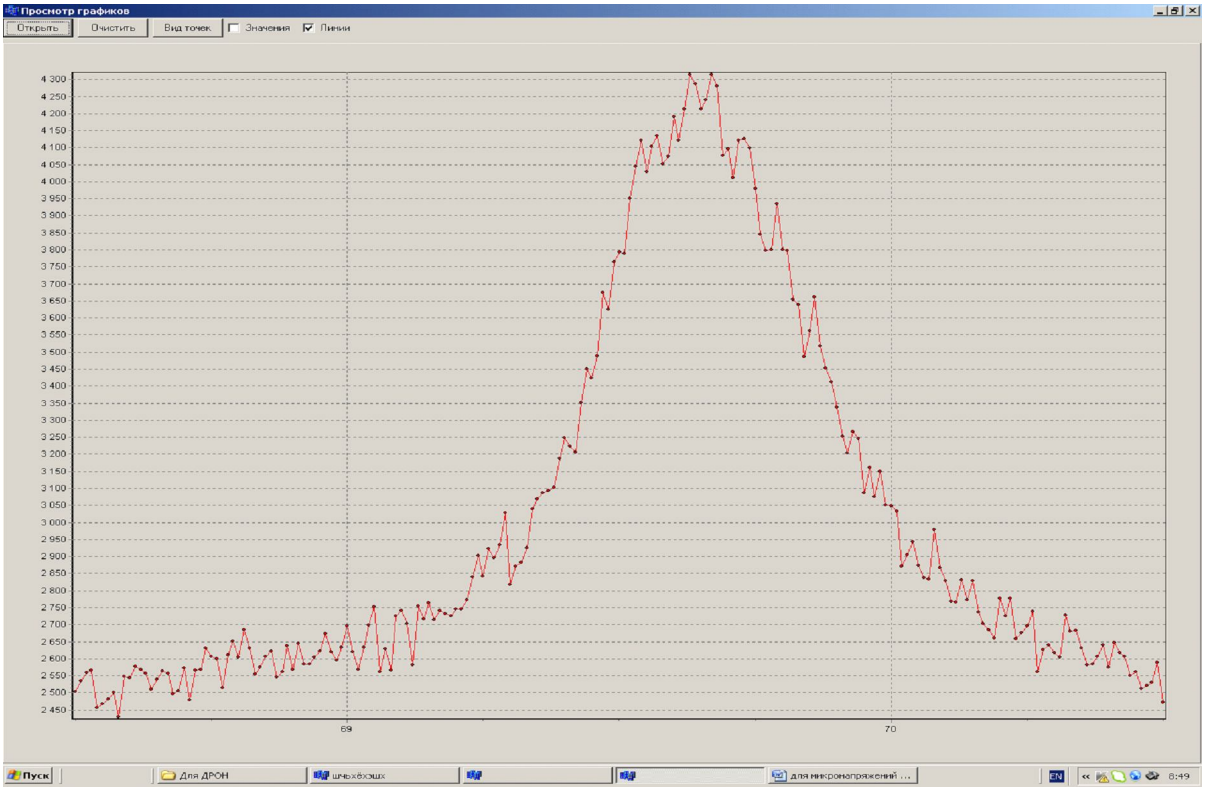


Рис. 3. Фрагмент дифрактограммы образца из ниобиевого сплава 5 ВМЦ,
после насыщения азотом 800° – 10 ч и отжигов 1,5 ч – 1000 °С и 1 ч – 1200 °С. Линия $(211)_{\alpha}$

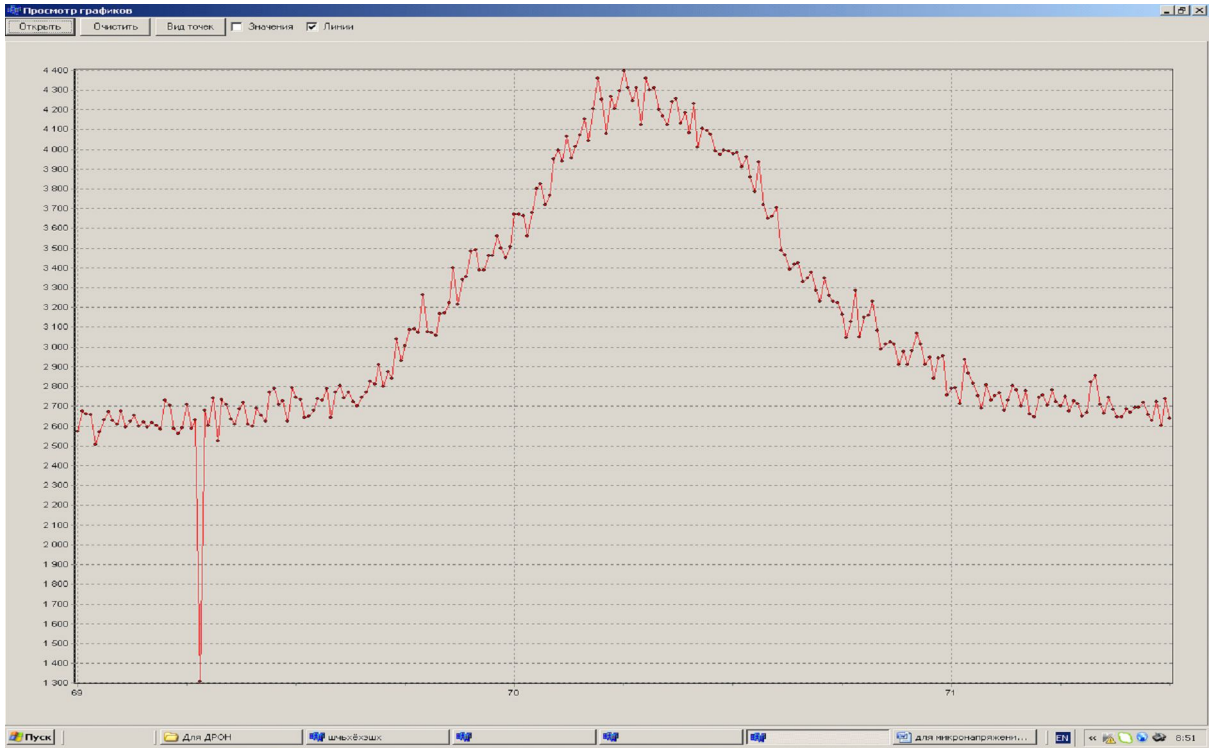


Рис. 4. Фрагмент дифрактограммы образца из ниобиевого сплава 5 ВМЦ в исходном состоянии.
Линия $(211)_{\alpha}$

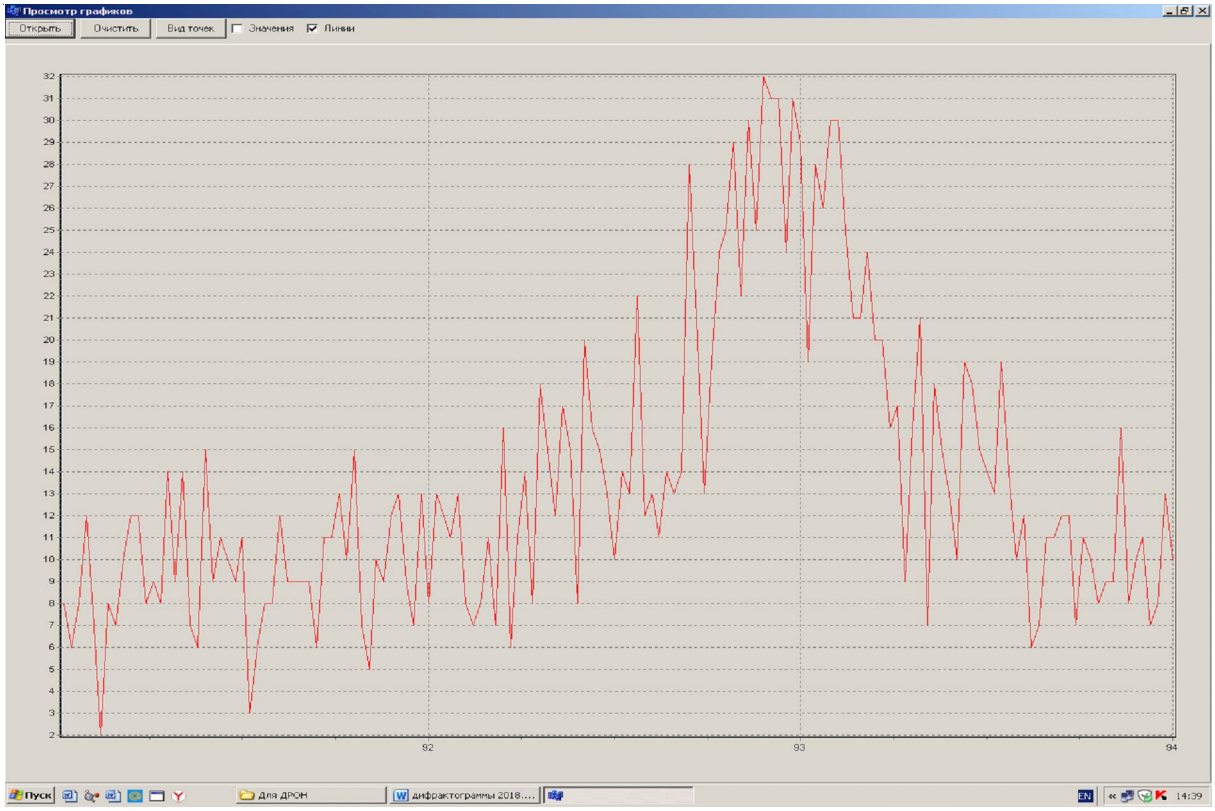


Рис. 5. Фрагмент дифрактограммы образца из ниобиевого сплава 5 ВМЦ, после насыщения азотом 550° – 8 ч и отжигов 1 ч – 1000 °С и 1,5 ч – 1200 °С. Линия $(311)_{\alpha}$. Линия $(211)_{\alpha}$

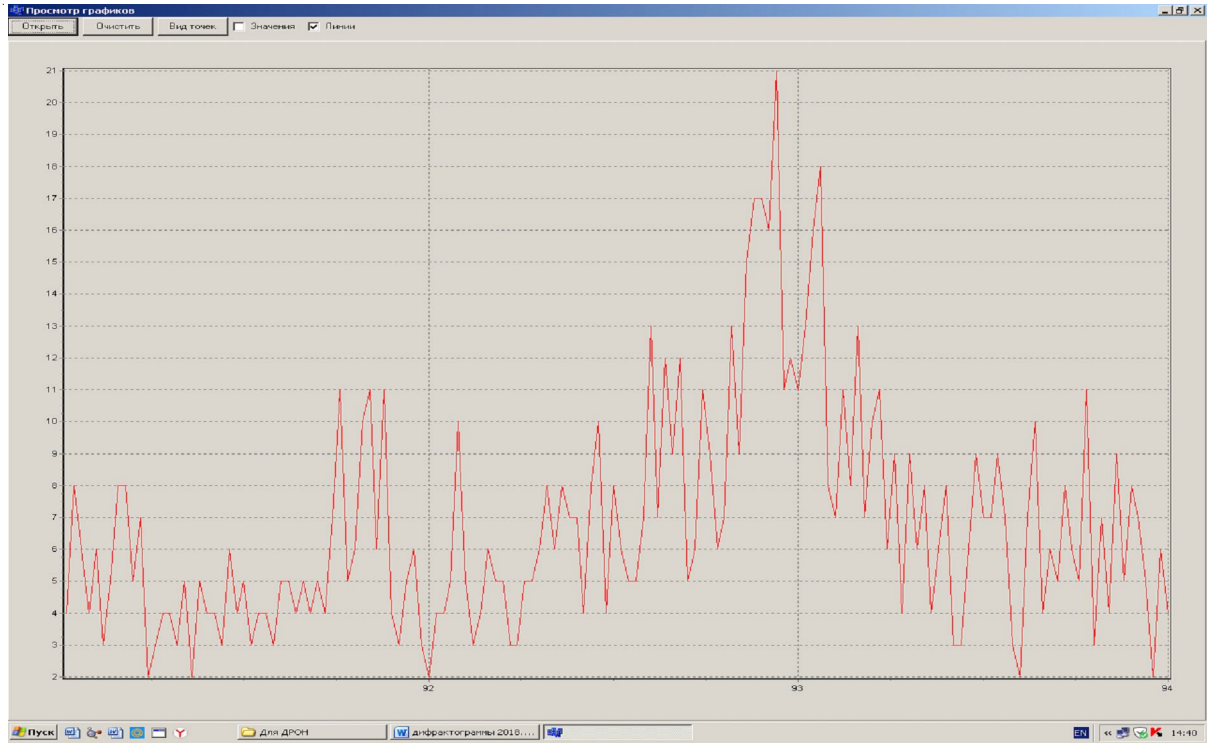


Рис. 6. Фрагмент дифрактограммы образца из ниобиевого сплава 5 ВМЦ в исходном состоянии. Линия $(211)_{\alpha}$

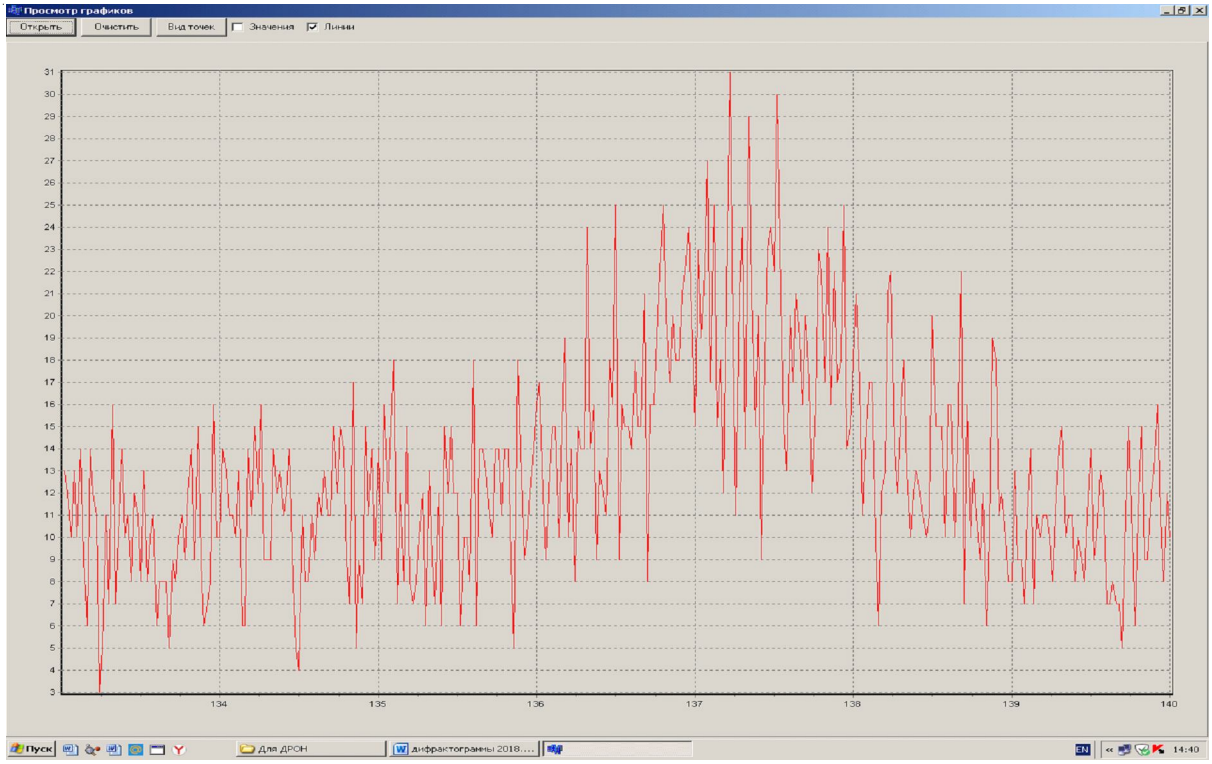


Рис. 7. Фрагмент дифрактограммы образца из ниобиевого сплава 5 ВМЦ,
после насыщения азотом 550° – 8 ч и отжигов 1 ч – 1000 °С и 1,5 ч – 1200 °С. Линия $(311)_{\alpha}$

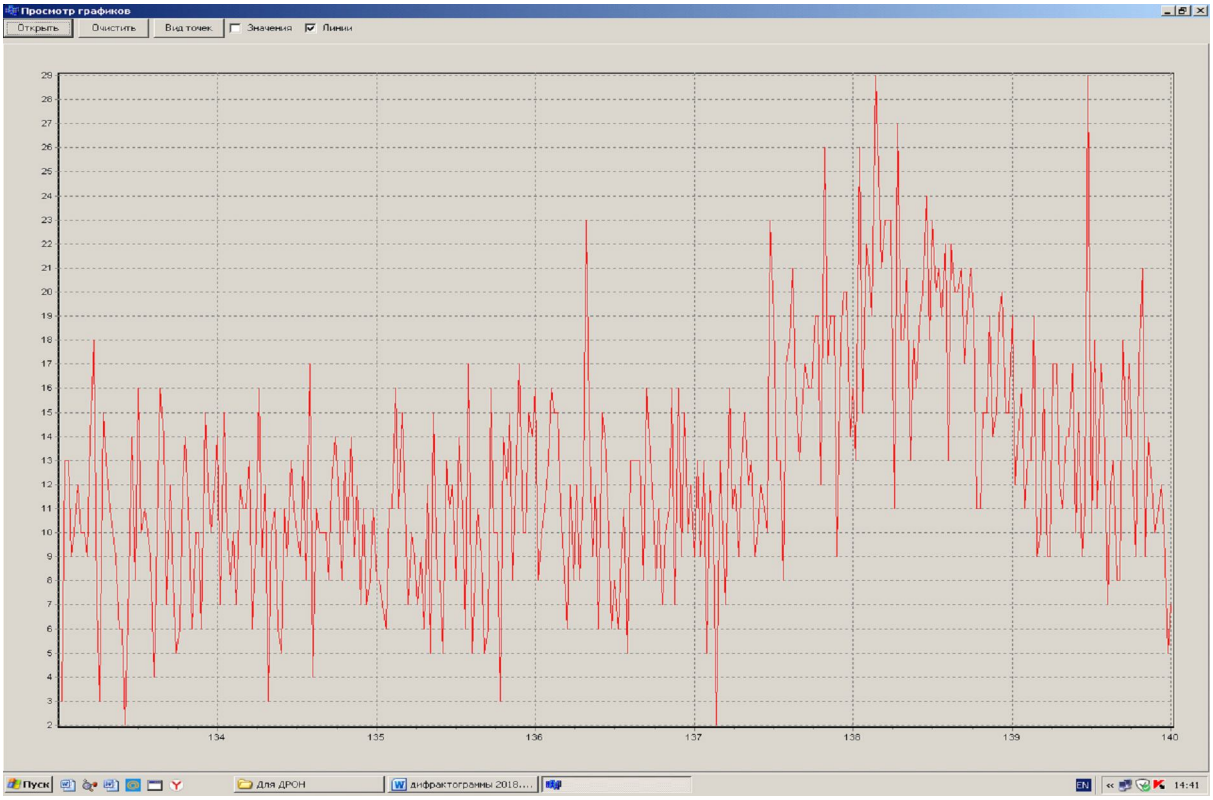


Рис. 8. Фрагмент дифрактограммы образца из ниобиевого сплава 5 ВМЦ в исходном состоянии.
Линия $(311)_{\alpha}$

Результаты расчета плотности дислокаций, рассчитанной по различным методикам

Режим насыщения	Плотность дислокаций, $\rho = 8\varepsilon^2/b^2$	Плотность дилокаций $\rho_{\perp} = 0{,}8\frac{ctg^2\theta_2 \ \beta_2^2}{b^2}$	Плотность дислокаций $\rho = \left(\frac{Lf}{b^2}\right) ctg^2\theta_2\beta_2^2$	Плотность дислокаций $N = K_0 ctg^2\Theta$
800^0С-10ч + вакуумный отжиг 1000^0С-1,5ч 1200^0С-1ч.	$140 \cdot 10^{14}$м$^{-2}$	$130 \cdot 10^{14}$м$^{-2}$	$126 \cdot 10^{14}$м$^{-2}$	$171 \cdot 10^{14}$м$^{-2}$
550^0С-10ч.+ вакуумный отжиг 1200^0С-1,5ч.	$199 \cdot 10^{14}$м$^{-2}$	$161 \cdot 10^{14}$м$^{-2}$	$220 \cdot 10^{14}$м$^{-2}$	$192 \cdot 10^{14}$м$^{-2}$

Примечание. В таблице представлены средние значения из 3–5 измерений.

Различия в данных иногда могут быть связаны с влиянием на уширение дифракционных линий некоторой величины микроискажений кристаллической решетки.

По литературным [3] и экспериментальным данным рентгеноструктурного анализа была построена диаграмма зависимости значений плотности дислокаций от режимов насыщения (рис. 9) для ниобиевого сплава 5 ВМЦ, которая позволяет определить возможные режимы процесса внутреннего азотирования для данного сплава.

Выводы

1. Выполненные исследования позволяют рассмотреть возможность упрочнения жаропрочных ниобиевых сплавов, связанные с использованием особенностей ультрамелкозернистой структуры с ультрадисперсными нитридами в рамках реализации дислокационной ячеисто-нитридной структуры, в которой растворимость азота может превышать равновесные значения.

2. Полученные экспериментальные результаты дают возможность оценить влияние плотности дислокаций, как одного из параметра тонкой структуры на возможные режимы внутреннего азотирования.

СПИСОК ЛИТЕРАТУРЫ

1. Горелик, С. С. Рентгенографический и электронно-оптический анализ / С. С. Горелик, Ю. А. Скаков, Л. Н. Расторгуев. – М. : МИСИС, 2002. – 360 с.

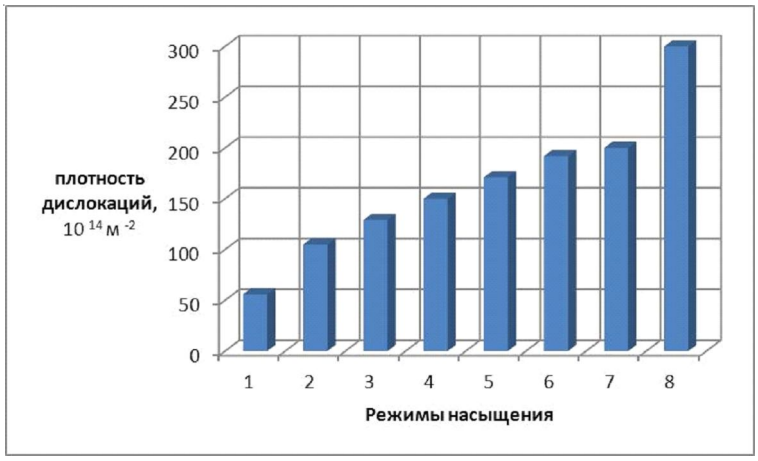


Рис. 9. Зависимость значений плотности дислокаций от режимов внутреннего азотирования. По оси абсцисс введены следующие обозначения:

1 – насыщение при 550 °С – 10 ч; *2* – насыщение 1000 °С – 1 ч; *3* – насыщение 800 °С – 8 ч; *4* – насыщение 800 °С – 10 ч; *5* – насыщение 800 °С – 10 ч + вакуумный отжиг 1000 °С – 1,5 часа + вакуумный отжиг – 1200 °С – 1,5 ч; *6* – насыщение 700 °С – 20 ч; *7* – насыщение при 550 °С – 10 ч + вакуумный отжиг 1200 °С – 1, 5 ч; *8* – насыщение при 700 °С – 10 ч

2. Иванченко, А. В. Определение температурного порога рекристаллизации ниобиевого сплава 5 ВМЦ до и после внутреннего азотирования / А. В. Иванченко, Е. Е. Складнова, К. О. Смирнов // Вестник Волгоградского государственного университета. Серия 1, Математика. Физика. – 2000. – Вып. 5. – С. 107–110.

3. Иванченко, А. В. Создание клатратно-ячеистой структуры как способ упрочнения ниобиевых сплавов / А. В Иванченко, Е. Е. Складнова, К. О. Смирнов // Вестник Волгоградского государственного университета. Серия 1, Математика. Физика. – 1997. – Вып. 2. – С. 118–126.

4. Иванченко, А. В. Трибохимическое смещение температурного порога рекристаллизации ($T_{п.р.}$) сплавов / А. В. Иванченко, Е. Е. Складнова, К. О. Смирнов // Нелинейные процессы и проблемы самоорганизации в современном материаловедении : тез. докл. I Всерос. семинара, г. Москва, апр. 1997 г. – М. : Изд-во МГУ, 1997. – С. 90.

5. Кашин, Д. С. Защитные покрытия для жаропрочных сплавов на основе ниобия / Д. С. Кашин, П. А. Стехов // Электронный научный журнал «ТРУДЫ ВИАМ». – 2015. – № 6. – С. 3–6.

6. Кристаллография, рентгенография и электронная микроскопия / Я. С. Уманский, Ю. А. Скаков, А. Н. Иванов, Л. Н. Расторгуев. – М. : Металлургия, 1982. – 632 с.

7. Оспенникова, О. Г. Тугоплавкие сплавы для новой техники / О. Г. Оспенникова, В. Н. Подъячев, Ю. В. Столянков // Электронный научный журнал «Труды ВИАМ». – 2016. – № 10. – С. 55–64.

8. Хоникомб, Р. Пластическая деформация металлов / Р. Хоникомб. – М. : Мир, 1972. – 408 с.

REFERENCES

1. Gorelik S.S., Skakov Yu.A., Rastorguev L.N. *Rentgenograficheskij i elektronno-opticheskij analiz* [X-ray and Electron-Optical Analysis]. Moscow, MISIS Publ., 2002. 360 p.

2. Ivanchenko A.V., Skladnova E.E., Smirnov K.O. Opredelenie temperaturnogo poroga rekristallizacii niobievogo splava 5 VMC do i posle vnutrennego azotirovaniya [Determination of the Temperature Threshold of Recrystallization of Niobium Alloy 5 VMC Before and After Internal Nitriding]. *Vestnik VolGU. Seriya 1. Matematika. Fizika* [Mathematical Physics and Computer Simulation], 2000, iss. 5, pp. 107-110.

3. Ivanchenko A.V., Skladnova E.E., Smirnov K.O. Sozdanie klatratno-yacheistoj struktury kak sposob uprochneniya niobievyh splavov [Creation of a Clathrate-Cellular Structure as a Method of Strengthening Niobium Alloys]. *Vestnik VolGU. Seriya 1. Matematika. Fizika* [Mathematical Physics and Computer Simulation], 1997, iss. 2, pp. 118-126.

4. Ivanchenko A.V., Skladnova E.E., Smirnov K.O. Tribohimicheskoe smeshchenie temperaturnogo poroga rekristallizacii ($T_{p.r.}$) splavov [Tribochemical Displacement of the Temperature Threshold of Recrystallization (Tp.r.) of Alloys]. *Nelineynyye protsessy i problemy samoorganizatsii v sovremennom materialovedenii: tez. dokl. I Vseros. seminara, g. Moskva, apr. 1997 g.* Moscow, MGU Publ., 1997, p. 90.

5. Kashin D.S., Stekhov P.A. Zashchitnye pokrytiya dlya zharoprochnyh splavov na osnove niobiya [Protective Coatings for Heat-Resistant Niobium-Based Alloys]. *Elektronnyj nauchnyj zhurnal «TRUDY VIAM»*, 2015, no. 6, pp. 3-6.

6. Umanskij Ya.S., Skakov Yu.A., Ivanov A.N., Rastorguev L.N. *Kristallografiya, rentgenografiya i elektronnaya mikroskopiya* [Crystallography, X-ray Diffraction and Electron Microscopy]. Moscow, Metallurgiya Publ., 1982. 632 p.

7. Ospennikova O.G., Podyachev V.N., Stolyankov Yu.V. Tugoplavkie splavy dlya novoj tekhniki [Refractory Alloys for New Equipment]. *Elektronnyj nauchnyj zhurnal «Trudy VIAM»*, 2016, no. 10, pp. 55-64.

8. Honikomb R. *Plasticheskaya deformaciya metallov* [Plastic Deformation of Metals]. Moscow, Mir Publ., 1972. 408 p.

INVESTIGATION OF THE FINE STRUCTURE OF 5 VMC NIOBIUM ALLOY SAMPLES AFTER INTERNAL NITRIDING

Konstantin O. Smirnov

Senior Lecturer, Department of Forensic Science and Physical Materials Science,
Volgograd State University
priori@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. The paper considers the possibility of studying the fine structure of samples made of niobium alloy 5 VMC (grade 5B2MC-2), which underwent internal nitriding by X-ray diffraction analysis.The calculation of the dislocation density, which represents one of the parameters of the fine structure using various techniques, is shown. Its influence on the possible modes of internal nitriding is considered.

Key words: X-ray diffraction analysis, dislocation density, hardening of niobium alloys.

Журнал «НБИ технологии» издается для широкого ознакомления научной общественности с результатами современных исследований, посвященных вопросам развития инновационной деятельности, защиты объектов интеллектуальной собственности и ее коммерциализации, государственной политики в сфере управления инновациями, а также реализации инновационных технологий обучения.

Авторами «НБИ технологии» могут быть преподаватели, научные сотрудники и аспиранты высших учебных заведений и научно-исследовательских учреждений России, а также другие отечественные и зарубежные исследователи.

Уважаемые читатели!

Подписка на I полугодие 2021 года осуществляется
по «Объединенному каталогу. Пресса России. Газеты и журналы». Т. 1.
Подписной индекс 10384.

Стоимость подписки на I полугодие 2021 года 1 024 руб. 42 коп.
Распространение журнала осуществляется по адресной системе.

ТРЕБОВАНИЯ К СТАТЬЯМ, ПРЕДСТАВЛЯЕМЫМ В РЕДКОЛЛЕГИЮ ЖУРНАЛА «НБИ ТЕХНОЛОГИИ»

1. Материалы представляются на бумажном и электронном носителях по адресу: 400062, г. Волгоград, просп. Университетский, 100, Волгоградский государственный университет – главному редактору Запороцковой Ирине Владимировне или высылаются по электронной почте на адреса: vestnik10@volsu.ru.

Обязательно наличие сопроводительного письма, в котором должны содержаться следующие пункты: гарантия оригинальности статьи, отсутствия в ней недостоверных данных и плагиата; обязательство не подавать данный материал в другой журнал; информация о наличии/отсутствии потенциального конфликта интересов с членами редколлегии; данные о финансировании исследования (с пометкой об их конфиденциальности или необходимости опубликования); согласие с принципами, изложенными в разделе «Издательская этика» журнала (https://ti.jvolsu.com/index.php/publishing-ethics-ru).

Для российских авторов (аспирантов и соискателей ученой степени кандидата наук) необходимо дополнительно представить рекомендацию, подписанную научным руководителем и заверенную печатью учреждения.

2. Правила оформления статей.

Объем статьи не должен превышать 1 п. л.

Каждая статья должна включать следующие элементы издательского оформления:

1) Индексы УДК и ББК.
2) Заглавие. Подзаголовочные данные (на русском и английском языках).
3) Имя, отчество, фамилия автора; ученое звание, ученая степень; контактная информация (место работы/учебы и должность автора, полный почтовый адрес организации, телефон, e-mail) на русском и английском языках.
4) Аннотация на русском языке и авторское резюме (Abstract) на английском языке.
5) 5–8 ключевых слов или словосочетаний (на русском и английском языках).
6) Текст статьи.
7) Список литературы на русском языке, оформленный в соответствии с ГОСТ Р 7.1-2003, и References – список литературы на английском языке (латинским шрифтом), оформленный в соответствии с требованиями редакции. При необходимости – примечания, приложения.

2.1. Требования к авторским оригиналам на бумажном и электронном носителях:

1) Поля по 2 см с каждой стороны.
2) Нумерация страницы по центру внизу.
3) Шрифт Times New Roman, кегль 14, междустрочный интервал 1,5.
4) Файл должен быть создан в программе «Microsoft Word» и сохранен с расширением *.rtf; имя файла должно быть набрано латиницей и отражать фамилию автора.

2.2. Оформление библиографических ссылок и примечаний:

1) Библиографические ссылки на пристатейный список литературы должны быть оформлены с указанием в строке текста в квадратных скобках цифрового порядкового номера источника и через запятую номеров соответствующих страниц.
2) Пристатейный список литературы, озаглавленный как «Список литературы», составляется в алфавитном пронумерованном порядке. Он должен быть оформлен согласно ГОСТ 7.1–2003 с указанием обязательных сведений библиографического описания.

3. После получения материалов рукопись направляется на рецензирование. Решение о публикации статей принимается редакционной коллегией после рецензирования. Редакция оставляет за собой право отклонить или отправить представленные статьи на доработку на основании соответствующих заключений рецензентов. После получения положительной рецензии редакция уведомляет авторов о том, что статья принята к опубликованию, а также направляет замечания рецензентов и редакторов, в соответствии с которыми необходимо исправить или дополнить статью. В случае отказа в публикации статьи редакция представляет автору мотивированный отказ.

Полнотекстовые версии опубликованных статей и их метаданные (аннотации, ключевые слова, информация об авторах на русском и английском языках, список литературы) будут размещены в свободном доступе в Интернете на официальном сайте издания, на платформе Научной электронной библиотеки eLIBRARY.RU и других реферативных баз данных.

4. Более подробно с требованиями к статьям можно ознакомиться на страничке Издательства на сайте Волгоградского государственного университета: https://www.volsu.ru – и сайте журнала: https://ti.jvolsu.com.