Правовая информатика

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ
№ 3, 2021 г.
Выходит 4 раза в год

Зарегистрировано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций
Свидетельство № 015372 от 01.11.1996 г.

Журнал входит в систему Российского индекса научного цитирования (РИНЦ) и международную систему идентификации научных публикаций CrossRef (DOI).

Учредитель и издатель:
Федеральное бюджетное учреждение «Научный центр правовой информации при Министерстве юстиции Российской Федерации»

Отпечатано в РИО НЦПИ при Минюсте России.
Печать цветная цифровая.
Подписано в печать 05.10.2021 г.
Общий тираж 100 экз. Цена свободная.

Адрес редакции:
125437, Москва, Михалковская ул., 65, стр.1
Телефон: +7 (495) 539-25-29
E-mail: inform360@yandex.com
Требования, предъявляемые к рукописям, размещены на сайте
http://uzulo.su/prav-inf

СОДЕРЖАНИЕ

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ

КАЧЕСТВО СИСТЕМАТИЗАЦИИ НАУЧНЫХ СПЕЦИАЛЬНОСТЕЙ В РОССИЙСКОЙ НОМЕНКЛАТУРЕ 2021 ГОДА
Омельченко В.В. 4

ИНФОРМАЦИОННЫЕ И АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ И СЕТИ

ИНТЕЛЛЕКТУАЛЬНЫЕ ПРОГРАММНО-АППАРАТНЫЕ РЕШЕНИЯ ДЛЯ АВТОМАТИЗИРОВАННЫХ ОПТИКО-ЭЛЕКТРОННЫХ СИСТЕМ РЕАЛЬНОГО ВРЕМЕНИ
Гаврилов Д.А. 14

ИНФОРМАЦИОННЫЕ И ЭЛЕКТРОННЫЕ ТЕХНОЛОГИИ В ПРАВОВОЙ СФЕРЕ

ИНФОРМАЦИОННЫЕ И ПРОГРАММНЫЕ АСПЕКТЫ РАЗРАБОТКИ И ПРИМЕНЕНИЯ СМАРТ-КОНТРАКТОВ
Федосеев С.В. 25

ИНФОРМАЦИОННАЯ И КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

МЕТОДЫ И ПРОЦЕДУРЫ ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В ЭРГАСИСТЕМАХ
Ловцов Д.А. 34

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, РЕАЛИЗУЮЩЕЕ АЛГОРИТМ ШАМИРА В СТОЙКИХ ЧАСТНЫХ КРИПТОСИСТЕМАХ
Гриднев В.А., Селиванов А.Ю. 50

СПОСОБЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ АНОНИМНОСТИ В ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ
Карпов Д.С., Ибрагимова З.А. 60

ПРАВОВЫЕ РЕЖИМЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ

МОДЕЛИРОВАНИЕ АДАПТАЦИИ ЭЛЕКТРОННЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ ДЛЯ СЛАБОВИДЯЩИХ И НЕЗРЯЧИХ ПОЛЬЗОВАТЕЛЕЙ
Алексеев В.В., Дубровина О.В. 68

Подписка на журнал осуществляется в почтовых отделениях по каталогу «Пресса России». Подписной индекс: 34077

LEGAL INFORMATICS

RESEARCH AND PRACTICE JOURNAL
2021, No. 3
The journal is published quarterly.

Registered by the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications
Registration Certificate No. 015372
of the 1st of November 1996.

The journal is registered in the Russian Science Citation Index (RINTs) and CrossRef, the official Registration Agency of the International Digital Object Identifier (DOI) Foundation

Founder and publisher:
Federal State-Funded Institution "Scientific Centre for Legal Information under the Ministry of Justice of the Russian Federation"

Printed by the Printing and Publication Division of the Scientific Centre for Legal Information under the Ministry of Justice of the Russian Federation.
Printed in digital colour. Approved for print on the 5th of October, 2021.
Number of items printed: 100. Free price.

Postal address:
Mikhalkovskaya str., bld. 65/1,
125 438, Moscow, Russia
Telephone: +7 (495) 539-25-29
E-mail: inform360@yandex.com
Guidelines for preparing manuscripts for publication can be found on the website
http://uzulo.su/prav-inf

CONTENTS

INFORMATION SUPPORT FOR LEGAL REGULATION

THE QUALITY OF SYSTEMATISATION OF SCIENTIFIC SPECIALTIES IN THE 2021 RUSSIAN NOMENCLATURE
Victor Omel'chenko *4*

INFORMATIONAL AND AUTOMATED SYSTEMS AND NETWORKS

INTELLIGENT SOFTWARE AND HARDWARE SOLUTIONS FOR AUTOMATED REAL TIME ELECTRONIC OPTICAL SYSTEMS
Dmitrii Gavrilov *14*

INFORMATION AND ELECTRONIC TECHNOLOGIES IN THE LEGAL SPHERE

INFORMATION AND SOFTWARE ASPECTS OF THE DEVELOPMENT AND APPLICATION OF SMART CONTRACTS
Sergei Fedoseev *25*

INFORMATION AND COMPUTER SECURITY

METHODS AND PROCEDURES FOR ENSURING INFORMATION SECURITY IN ERGASYSTEMS
Dmitrii Lovtsov *34*

SOFTWARE IMPLEMENTING THE SHAMIR ALGORITHM IN STRONG PRIVATE CRYPTOSYSTEMS
Viktor Gridnev, Aleksandr Selivanov *50*

WAYS AND MEANS TO ENSURE ANONYMITY IN THE GLOBAL INTERNET NETWORK
Dmitrii Karpov, Zaira Ibragimova *60*

LEGAL REGIMES OF INFORMATION RESOURCES

ELECTRONIC INFORMATION RESOURCES ADAPTATION MODELLING FOR VISUALLY IMPAIRED AND BLIND USERS
Vladimir Alekseev, Oksana Dubrovina *68*

The journal can be subscribed to at post offices through the Press of Russia (Pressa Rossii) Catalogue. Publication index: 34077

КАЧЕСТВО СИСТЕМАТИЗАЦИИ НАУЧНЫХ СПЕЦИАЛЬНОСТЕЙ В РОССИЙСКОЙ НОМЕНКЛАТУРЕ 2021 ГОДА

Омельченко В.В.*

***Ключевые слова**: государственная политика, недостатки, номенклатура, классификация, контроль, научное направление, научная специальность, систематизация, ученые степени.*

Аннотация.

Цель работы: оценка качества систематизации и классификации в новой «Номенклатуре научных специальностей, по которым присуждаются ученые степени», введенной Приказом Минобрнауки России от 24 февраля 2021 года № 118.

Методы: комплексные аналитические и экспертные методы систематизации и общей теории классификации, структурно-логический анализ.

Результаты: с системных позиций проведена экспертиза новой «Номенклатуры научных специальностей, по которым присуждаются ученые степени» с точки зрения выполнения базовых требований к классификации и систематизации объектов, процессов или явлений реальности, в том числе проведен структурно-логический анализ основных изменений в новой Номенклатуре, оценка качества основных классификационных схем, а также смысловой анализ систематизации предложенных научных специальностей; отмечена положительная динамика в устранении ряда выявленных в 2018—2020 гг. недостатков, противоречий и других аномалий (неадекватности) действовавшей до 24 февраля 2021 г. «Номенклатуры научных специальностей, по которым присуждаются ученые степени»; рассмотрены основные недостатки новой Номенклатуры и даны рекомендации по их устранению.

DOI: 10.21681/1994-1404-2021-3-04-13

Введение

Действующая до 24 февраля 2021 г. «Номенклатура научных специальностей, по которым присуждаются ученые степени» (далее — старая Номенклатура) неоднократно подвергалась предметной критике в течение 2018—2020 гг., которая изложена в ряде авторских публикаций, в том числе и на страницах нашего журнала [12—14].

На основании рекомендации Высшей аттестационной комиссии Приказом Минобрнауки РФ от 24 февраля 2021 г. № 118 утверждена новая «Номенклатура научных специальностей, по которым присуждаются ученые степени» (далее — новая Номенклатура)[1]. Подготовка новой редакции Номенклатуры проводилась в соответствии с поручением Президента РФ от 28 марта 2020 г. № Пр-589.

При разработке новой Номенклатуры было произведено *укрупнение* научных специальностей. Цель нововведений — создание предпосылок для концентрации усилий научного сообщества на развитии перспективных научных направлений и расширение междисциплинарных исследований.

В настоящей статье мы не будем касаться вопроса достижения целей разработки новой Номенклатуры, а сосредоточимся на *оценке качества* систематизации и классификации в новой «Номенклатуре научных специальностей, по которым присуждаются ученые степени». Проведем также анализ степени устранения в новой редакции Номенклатуры основных замечаний, недостатков и аномалий, выявленных в старой Номенклатуре, действовавшей до 24 февраля 2021 года.

Для достижения поставленных целей используем комплексные аналитические и экспертные методы систематизации и общей теории классификации объектов, процессов и явлений реальности [4—7, 12—14].

[1] Приказ Минобрнауки РФ от 24 февраля 2021 г. № 118 «Об утверждении Номенклатуры научных специальностей, по которым присуждаются ученые степени, и внесении изменения в Положение о совете по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук, утв. Приказом Минобрнауки РФ от 10 ноября 2017 г. № 1093».

* ***Омельченко Виктор Валентинович,*** *доктор технических наук, профессор, заслуженный деятель науки и техники Российской Федерации, государственный советник Российской Федерации 1-го класса, советник секретариата научно-технического совета АО «ВПК «НПО машиностроения», г. Москва, Российская Федерация.*

E-mail: omvv@yandex.ru

Анализ новой номенклатуры с точки зрения введенных изменений классификационной структуры, логики и смыслов

В Федеральном законе от 23 августа 1996 г. № 127-ФЗ[2] определено: «*Ученые степени кандидата наук, доктора наук присуждаются по научным специальностям в соответствии с номенклатурой, утвержденной федеральным органом исполнительной власти, осуществляющим функции по выработке государственной политики и нормативно-правовому регулированию в сфере научной и научно-технической деятельности. Указанная номенклатура является обязательной для всех ученых степеней, присуждаемых в рамках государственной системы научной аттестации*».

Традиционную оценку состава и изменений новой утвержденной «Номенклатуры научных специальностей, по которым присуждаются ученые степени» в научной среде и в прессе можно свести к следующему.

Согласно новой Номенклатуре, количество групп научных специальностей сократилось с 52 до 34 (-35%), специальностей — с 430 до 351 (-18,4%). При этом состав новой Номенклатуры пополнила 21 специальность, не имеющая принадлежности к уже существующим группам. Кроме того, в новой Номенклатуре появились *четыре* новых группы: компьютерные науки и информатика, биотехнология, недропользование и горные науки, когнитивные науки. По одному новому профилю получили группы специальностей по теологии, клинической медицине, строительству и архитектуре.

Такие сведения дают лишь общее представление о проведенной работе по изменению состава новой Номенклатуры. Однако оценить качество новой «Номенклатуры научных специальностей, по которым присуждаются ученые степени» на основе такого подхода не представляется возможным.

В соответствии с требованиями общей теории классификации [12] проведем более глубокий анализ сущности проведенных изменений, а также оценим качество новой Номенклатуры научных специальностей. Для этого проведем рассмотрение по двум направлениям:

1) структурно-логический анализ основных изменений в новой Номенклатуре;

2) анализ качества основных классификационных схем в новой Номенклатуре на предмет соответствия требованиям систематизации и классификации и смысловой анализ систематизации предложенных научных специальностей.

Анализ классификационной структуры новой Номенклатуры научных специальностей и основных ее новшеств

Структура новой Номенклатуры (как и предыдущей Номенклатуры) осталась трехуровневой, однако ее содержательная часть несколько изменилась:

1 уровень: **было** — группы научных специальностей; **стало** — области (классы) науки;

2 уровень: **было** — подгруппы научных специальностей, входящих в группы; **стало** — группы (подклассы) научных специальностей, входящих в области (классы) науки;

3 уровень: **было** — научные специальности, входящие в соответствующие подгруппы и группы; **стало** — научные специальности, входящие в соответствующие группы и области науки.

Предложенные изменения в содержательной части позволили внести ряд позитивных изменений в новой Номенклатуре, в том числе устранить очевидные грубые недостатки систематизации и классификации, приведенные в [12—14] (см. *таблицу*):

1) значительно сократить — до пяти классов (областей наук) — первый уровень классификации из 26 групп в старой Номенклатуре;

2) устранить «пустые» или без наименований 13 из 26 групп научных специальностей (1-я, 3-я, 4-я, 5-я, 6-я, 10-я, 11-я, 14-я, 15-я, 16-я, 18-я, 20-я, 21-я).

Представленные в таблице сведения о характере внесенных изменений в старой Номенклатуре (как **было**) и новой Номенклатуре (как **стало**) позволяет провести сравнительный анализ изменений и оценить масштаб проведенной работы.

Для анализа сущности представленных изменений старой Номенклатуры и более предметного рассмотрения классификационной схемы новой «Номенклатуры научных специальностей, по которым присуждаются ученые степени», представим классификационную схему последней с выделением новой группы специальностей «***Компьютерные науки и информатика***» (*рис*. 1).

Рассматриваемое на рисунке направление (ветвь) классификации и его классификационные элементы (классы, подклассы, объекты) приведены на зеленом фоне, означающем «правильность» (обоснованность) проведенной классификации. Обратим внимание на *первый* уровень представленной классификации, на котором выделено пять классов (областей наук). Перекрывают ли эти пять классов или областей наук новой Номенклатуры исходное множество научных специальностей разных областей науки, по которым присуждаются ученые степени? Другими словами, на этом уровне систематизации выполнено ли требование полноты декомпозиции исходного множества классификации?

Конечно, обеспечить выполнение этого требования оказывается не так просто даже для работников от науки. Ну, не получается, так введите еще один запасной или шестой класс (область других наук), те науки, которые не попадают в первые пять классов или попадают с нарушением требований классификации. А такие «не вписывающиеся» в Номенклатуру области науки, несомненно, проявятся уже завтра, если сегодня их еще нельзя «увидеть» или предвидеть.

Таким образом, анализ сущности представленных изменений старой Номенклатуры, с *одной* стороны, и рассмотрение новой классификационной схемы

[2] Федеральный закон от 23 августа 1996 г. № 127-ФЗ «О науке и государственной научно-технической политике» // СПС «КонсультантПлюс».

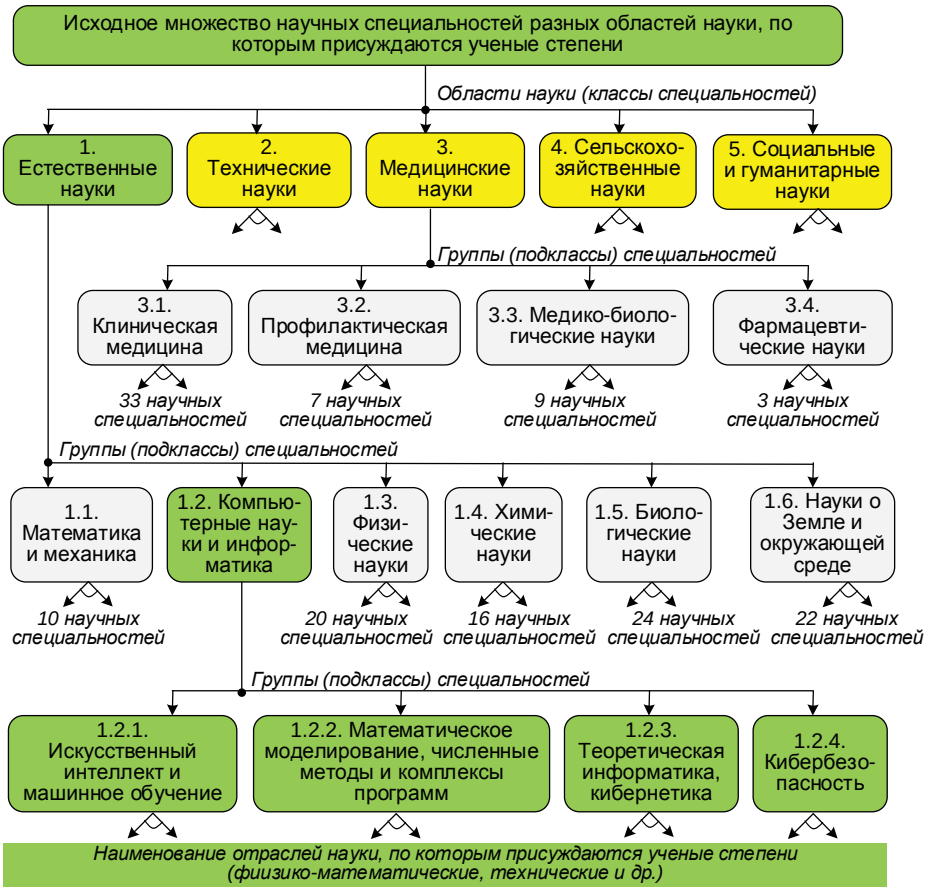

Рис. 1. Классификационная схема новой «Номенклатуры научных специальностей, по которым присуждаются ученые степени» и новой группы специальностей «Компьютерные науки и информатика»

новой Номенклатуры, с *другой* стороны, показывает значительные улучшения структурно-классификационных и смысловых сущностей проведенной работы.

В целом с учетом ранее выявленных и опубликованных ошибок и недостатков предыдущей Номенклатуры научных специальностей [12—14] можно сделать следующие *выводы*:

1. Устранены системные грубые ошибки (нарушения, аномалии, неадекватности) классификации научных специальностей, в том числе:

совмещение с предметно-ориентированными подгруппами научных специальностей 5-й группы старой Номенклатуры с универсальной 13-й подгруппой ***«Информатика, вычислительная техника и управление»***;

включение как в 5-ю предметно-ориентированную группу, так и в 13-ю подгруппу универсальную и инвариантную предметным областям научную специальность ***«Системный анализ, управление и обработка информации»***.

2. Устранены на первом и втором уровнях классификации «пустые» места старой систематизации (из 27 подгрупп научных специальностей отсутствует пять: № 3, 6, 10, 15, 24 в старой Номенклатуре);

3. Устранен дисбаланс по группам и подгруппам научных специальностей путем сокращения: количества групп научных специальностей с 52 до 34, специальностей — с 430 до 351.

4. Улучшилась классификационная структура новой Номенклатуры, прежде всего за счет:

пополнения более 20 специальностей, не имеющих принадлежности к уже существующим группам;

введения в новую Номенклатуру новых групп (всего четыре) научных специальностей.

Таким образом, в новой «Номенклатуре научных специальностей, по которым присуждаются ученые степени» по сравнению со старой Номенклатурой устранены многочисленные нарушения, недостатки и недоработки, выявленные в 2019 — 2020 гг. [12—14].

Вместе с тем, несмотря на положительную тенденцию по устранению рассмотренных недоработок, следует отметить и недостатки новой Номенклатуры.

Анализ качества основных классификационных схем новой Номенклатуры и смысловой анализ систематизации предложенных научных специальностей

Анализ проведем на примере правомочности включения фундаментальной научной специальности «***Системный анализ, управление и обработка информации***» с кодом 1.2.1 в новую группу специальностей «Ком-

Таблица

Сравнительный анализ изменений в новой Номенклатуре научных специальностей

Шифр	Наименование области науки (класса) научных специальностей (было и стало)	Наименование группы (подкласса) научных специальностей (было и стало)
01.00.00	**Было:** 1-й класс — **наименование не определено.** **Стало: Естественные науки** — как область науки	**Было:** 1. Математика. 2. Механика. 3. Астрономия. 4. Физика. **Стало:** изменены наименования и введены еще две группы научных специальностей
02.00.00	**Было:** 2-й класс — Химия. **Стало: Технические науки** — как область науки	**Было: Группы не определены** (приведено 17 из 21 заявленных наименований научных специальностей). **Стало:** существенно изменены наименования групп научных специальностей под названную область науки
03.00.00	**Было:** 3-й класс — **наименование не определено**. **Стало: Медицинские науки** — как область науки	**Было:** 1. Физико-химическая биология. 2. Общая биология. 3. Физиология. **Стало:** существенно изменены наименования групп научных специальностей под названную область науки
04.00.00	**Было:** 4-й класс — **наименование не определено**. **Стало: Сельскохозяйственные науки — как область науки**	**Было: Группы не определены**. **Стало:** существенно изменены наименования групп научных специальностей под названную область науки
05.00.00	**Было:** 5-й класс — **наименование не определено**. **Стало: Социальные и гуманитарные науки — как область науки**	**Было:** 1. Инженерная геометрия и компьютерная графика. 2. Машиностроение и машиноведение. 3. **Не определено.** 4. Энергетическое, металлургическое и химическое машиностроение. 5. Транспортное, горное и строительное машиностроение. 6. **Не определено.** 7. Авиационная и ракетно-космическая техника. 8. Кораблестроение. 9. Электротехника. 10. **Не определено.** 11. Приборостроение, метрология и информационно-измерительные приборы и системы. 12. Радиотехника и связь. 13. Информатика, вычислительная техника и управление. 14. Энергетика. 15. **Не определено.** 16. Металлургия и материаловедение. 17. Химическая технология 18. Технология продовольственных продуктов. 19. Технология материалов и изделий. текстильной и легкой промышленности. 20. Процессы и машины агроинженерных систем. 21. Технология, машины и оборудование лесозаготовок, лесного хозяйства, деревопереработки и химической переработки биомассы дерева. 22. Транспорт. 23. Строительство и архитектура. 24. **Не определено.** 25. Документальная информация. 26. Безопасность деятельности человека. 27. Электроника. **Стало:** Сокращено до 12 групп научных специальностей, существенно изменены наименования групп научных специальностей под названную область науки.

06.00.00	**Было:** 6-й класс — **наименование не определено.** **Стало: Класс сокращен, его содержимое включено в новую группу научных специальностей новой Номенклатуры**	**Было:** 1. Агрономия. 2. Ветеринария и зоотехния. 3. Лесное хозяйство. 4. Рыбное хозяйство. **Стало:** указанные группы научных специальностей распределены по пяти областям науки
07.00.00	**Было:** История и археология. **Стало: 7-й класс сокращен, его содержимое включено в новую группу научных специальностей новой Номенклатуры**	**Было: Группы не определены** (приведено 7 из 15 заявленных наименований научных специальностей). **Стало:** указанные группы научных специальностей определены и распределены по пяти областям науки
08.00.00	**Было:** Экономика. **Стало: 8-й класс сокращен, его содержимое включено в новую группу научных специальностей новой Номенклатуры**	**Было: Группы не определены** (приведено 6 из 14 заявленных наименований научных специальностей). **Стало:** указанные группы научных специальностей определены и распределены по пяти областям науки
09.00.00	**Было:** Философия. **Стало: 9-й класс сокращен, его содержимое включено в новую группу научных специальностей новой Номенклатуры**	**Было: Группы не определены** (приведено 9 из 14 заявленных наименований научных специальностей). **Стало:** группы научных специальностей определены и распределены по областям науки
10.00.00	**Было:** 10 класс — **наименование не определено**. **Стало: Класс сокращен, его содержимое включено в новую группу научных специальностей новой Номенклатуры**	**Было:** 1. Литературоведение. 2. Языкознание. **Стало:** указанные группы научных специальностей распределены по областям науки
11.00.00	**Было:** 11 класс — **наименование не определено**. **Стало: Класс сокращен, его содержимое включено в новую группу научных специальностей новой Номенклатуры**	**Было: Группы не определены.** **Стало:** группы научных специальностей определены и распределены по пяти областям науки
12.00.00	**Было:** Юриспруденция **Стало: 12 класс сокращен, его содержимое включено в новую группу научных специальностей новой Номенклатуры**	**Было: Группы не определены** (приведено 12 из 15 заявленных наименований научных специальностей). **Стало:** группы научных специальностей определены и распределены по пяти областям науки
13.00.00	**Было:** Педагогика. **Стало: 13 класс сокращен, его содержимое включено в новую группу научных специальностей новой Номенклатуры**	**Было:** Группы не определены (приведено 6 из 8 заявленных наименований научных специальностей). **Стало:** группы научных специальностей определены и распределены по пяти областям науки
14.00.00	**Было:** 14 класс — **наименование не определено**. **Стало: Класс сокращен, его содержимое включено в новую группу научных специальностей новой Номенклатуры**	**Было:** 1. Клиническая медицина. 2. Профилактическая медицина. 3. Медико-биологические науки. 4. Фармация. **Стало:** группы научных специальностей распределены по пяти областям науки
15.00.00	**Было:** 15 класс — **наименование не определено**. **Стало: Класс сокращен, его содержимое включено в новую группу научных специальностей новой Номенклатуры**	**Было: Группы не определены** (наименования научных специальностей отсутствуют). **Стало:** группы научных специальностей определены и распределены по пяти областям науки
16.00.00	**Было:** 16 класс — **наименование не определено**. **Стало: Класс сокращен, его содержимое включено в новую группу научных специальностей новой Номенклатуры**	**Было: Группы не определены** (наименования научных специальностей отсутствуют). **Стало:** группы научных специальностей определены и распределены по пяти областям науки
17.00.00	**Было:** Искусствоведение. **Стало: Класс сокращен, его содержимое включено в новую группу научных специальностей новой Номенклатуры**	**Было: Группы не определены** (приведено 7 из 9 заявленных наименований научных специальностей). **Стало:** группы научных специальностей определены и распределены по пяти областям науки

18.00.00	**Было:** 18 класс — наименование не определено. **Стало: Класс сокращен, его содержимое включено в новую группу научных специальностей новой Номенклатуры**	**Было: Группы не определены** (наименования научных специальностей отсутствуют). **Стало:** группы научных специальностей определены и распределены по пяти областям науки
19.00.00	**Было:** Психология. **Стало: 19 класс сокращен, его содержимое включено в новую группу научных специальностей новой Номенклатуры**	**Было: Группы не определены** (приведено 10 из 13 заявленных наименований научных специальностей). **Стало:** группы научных специальностей определены и распределены по пяти областям науки
20.00.00.	**Было:** 20 класс — наименование не определено. **Стало: Класс сокращен, его содержимое включено в новую группу научных специальностей новой Номенклатуры**	**Было: Группы не определены** (наименования научных специальностей отсутствуют). **Стало:** группы научных специальностей определены и распределены по пяти областям науки
21.00.00	**Было:** 21 класс — **наименование не определено**. **Стало: Класс сокращен, его содержимое включено в новую группу научных специальностей новой Номенклатуры**	**Было: Группы не определены** (наименования научных специальностей отсутствуют). **Стало:** группы научных специальностей определены и распределены по пяти областям науки
22.00.00	**Было:** Социология. **Стало: 22 класс сокращен, его содержимое включено в новую группу научных специальностей новой Номенклатуры**	**Было: Группы не определены** (приведено 6 из 8 заявленных наименований научных специальностей). **Стало:** группы научных специальностей определены и распределены по пяти областям науки
23.00.00	**Было:** Политология. **Стало: 23 класс сокращен, его содержимое включено в новую группу научных специальностей новой Номенклатуры**	**Было: Группы не определены** (приведено 6 из 6 заявленных наименований научных специальностей). **Стало:** группы научных специальностей определены и распределены по пяти областям науки
24.00.00	**Было:** Культурология. **Стало: 24 класс сокращен, его содержимое включено в новую группу научных специальностей новой Номенклатуры**	**Было: Группы не определены** (приведено 2 из 3 заявленных наименований научных специальностей). **Стало:** группы научных специальностей определены и распределены по пяти областям науки
25.00.00	**Было:** Науки о земле. **Стало: 25 класс сокращен, его содержимое включено в новую группу научных специальностей новой Номенклатуры**	**Было: Группы не определены** (приведено 18 из 36 заявленных наименований научных специальностей). **Стало:** группы научных специальностей определены и распределены по пяти областям науки
26.00.00	**Было:** Теология. **Стало: 26 класс сокращен, его содержимое включено в новую группу научных специальностей новой Номенклатуры**	**Было: Группы не определены** (приведено одно наименование научной специальности). **Стало:** группы научных специальностей определены и распределены по пяти областям науки

пьютерные науки и информатика» с кодом 1.2. Для этого приведем классификационную схему (*рис.* 2) новой «Номенклатуры научных специальностей, по которым присуждаются ученые степени» с выделением новой группы специальностей «Информационные технологии и телекоммуникации». На рис. 2 направление (ветвь) классификации и его классификационные элементы (классы, подклассы, объекты) выделены соответствующими цветами фона: *зеленый* — правильно классифицировано, *красный* — неправильно классифицировано (объект классификации отнесен не к тому классу).

Рассмотрим наиболее существенные или системные недостатки новой Номенклатуры.

Первое: все начинается с названия; «как корабль назовешь, так он и поплывет» — этот знаковый образ работает в нашем субъективном и объективном мире. Название документа «номенклатура» — это иностранное слово, которое означает[3]:

1) совокупность или перечень названий, терминов, употребляющихся в какой-либо отрасли науки, искусства, техники и др.;

2) круг должностных лиц, назначение или утверждение которых относится к компетенции какого-либо вышестоящего органа.

[3] Словарь иностранных слов. 15-е изд., испр. М. : «Русский язык», 1988. 608 с.

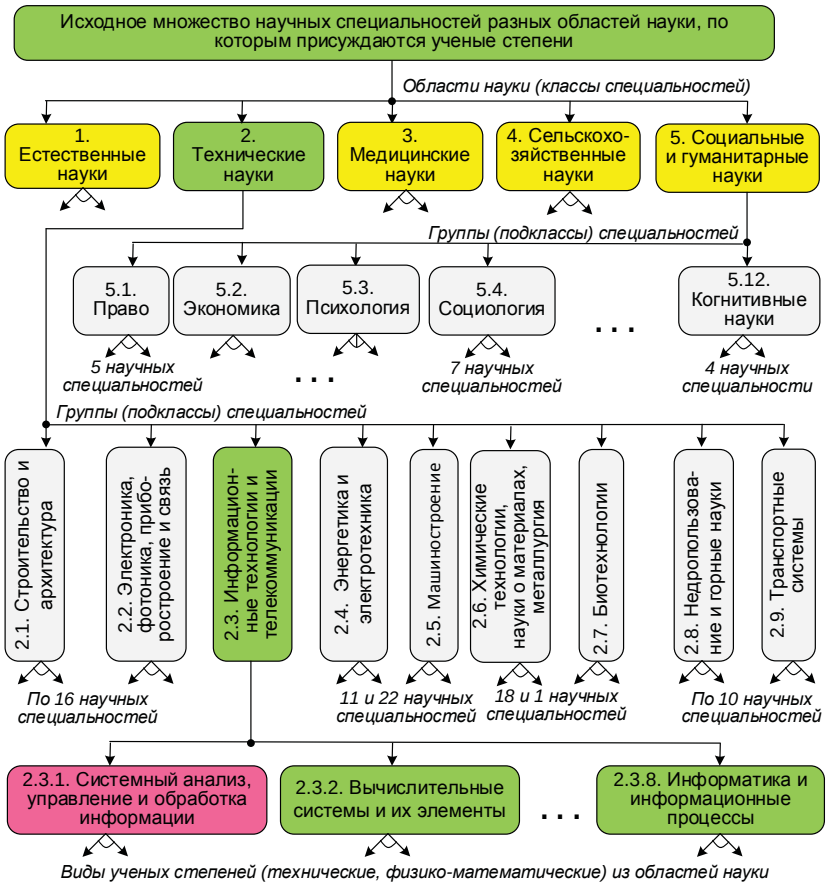

Рис. 2. Классификационная схема новой «Номенклатуры научных специальностей, по которым присуждаются ученые степени» с выделением новой группы специальностей «Информационные технологии и телекоммуникации»

В основных государственных документах, отражающих вопросы государственного управления научной и научно-технической деятельностью в Российской Федерации, в части государственного регулирования подготовкой и принятие системы научных специальностей определение иностранного слова «номенклатура» не приведено.

Если «Номенклатура научных специальностей, по которым присуждаются ученые степени» является просто «совокупностью или перечнем названий, терминов…», то какие могут быть вопросы к качеству систематизации или классификации научных специальностей. Таким образом, ответственные должностные лица уходят от ответственности. Но ведь разработанная классификационная система с соответствующими кодами, названная «Номенклатурой», по существу, номенклатурой не является.

Даже поверхностное знакомство с предложенной Номенклатурой позволяет неспециалисту в области *системного анализа* [4, 6] и государственного управления понять, что это не просто «совокупность или перечень названий, терминов…». Перед нами — определенная классификационная система научных специальностей, а это уже совсем другой уровень описания и представления знаний. Другими словами, перед нами не «номенклатура» или «перечень химических элементов», а «классификационная система Д. И. Менделеева».

Следовательно, рассматривать качество этой новой Номенклатуры надо с системных позиций, т. е., прежде всего, с позиций *теории классификации*, одно из первых *требований* которой следующее: «название сущности должно соответствовать ее содержанию» [8—11, 16]. Если этот принцип не соблюдается в таком важном направлении государственного управления и регулирования, значит, размывается суть используемых понятий и, как следствие, размывается ответственность за конечные результаты этого управления.

Второе: включение во 2-ю область науки «Технические науки» в группу «2.3. Информационные технологии и телекоммуникации» научной специальности «***2.3.1. Системный анализ, управление и обработка информации***» хотя и является шагом вперед по сравнению с предыдущей версией Номенклатуры, однако является далеко не лучшим классификационным решением, так как эта научная специальность неправильно классифицирована или отнесена не к тому классу.

Действительно, *системный анализ*, лежащий в основе любой систематизации и классификации как методология (наука) познания и как метод (инструмент) классификации (систематизации), обеспечивает универсальность и всеобщность данных сущностей, которые стоят над различными предметно-ориентированными сферами и научными специальностями.

Рис. 3. Классификационная схема верхнего уровня для перспективного варианта «Номенклатуры научных специальностей, по которым присуждаются ученые степени»

А разве для других областей науки, например, для естественных наук (код 1), медицинских наук (код 3), сельскохозяйственных наук (код 4), социальных и гуманитарных наук (код 5), да и вообще для любых других наук, не приведенных в Номенклатуре, системный анализ с систематизацией и классификацией объектов, процессов и явлений реальности не нужен?

В той же *философии* [2], в ее базовом разделе «познание реальности» (мира, действительности, бытия) — как обойтись без системного анализа, базирующегося на фундаментальных и универсальных свойствах и отношениях тождества и различия?

Вот почему предложенную новую Номенклатуру и ее классификационную схему нельзя рассматривать как законченную, а только как некоторый промежуточный этап формирования целостного и функционально достаточного перечня научных специальностей.

Именно на перспективу необходимо проводить дальнейший смысловой анализ систематизации предложенных научных специальностей, а отсюда и рассмотрение корректности и обоснованности включения предложенных специальностей в соответствующие области наук (классы) и подгруппы (подклассы) научных специальностей по признакам-основаниям *смысловой принадлежности*.

В этом плане мы опять возвращаемся к дискуссии о построении универсальной и тождественной (адекватной) реальности классификационной схеме научных специальностей, по которым присуждаются ученые степени. Один из вариантов такой классификационной схемы был рассмотрен ранее [14], поэтому пояснения к *рис*. 3 не приводятся.

Проведение такой работы имеет исключительную важность, ибо получение эффективно работающей системы научных специальностей, по которым присуждаются ученые степени, напрямую зависит от принятой классификационной схемы.

Исторические наглядные примеры такого *системного подхода*[4] или его игнорирования мы видим повсюду [1—8, 15]. Например, можно всю свою жизнь изучать химию и химические элементы, их свойства и характеристики, но при этом так и не понять сути этой научной специальности. А можно сразу изучить и понять главное в ней — *классификационную систему*[5] химических элементов Д. И. Менделеева, и тогда все становится на свои места.

Это значит: человек познающий, обучаемый познал главное — *систему* в этой научной специальности. Поэтому какие бы ни возникали в дальнейшем вопросы-ситуации по химии, которые суть элементы этой системы, для этого человека уже не будет проблем в понимании онтологии рассматриваемых сущностей.

Основная цель и предназначение устроения любой научной классификационной системы — системное упорядочение бесконечного множества различных объектов, процессов или явлений реальности в некоторую конечную систему классов. Это в полной мере относится и к рассматриваемой новой «Номенклатуре научных специальностей, по которым присуждаются ученые степени», структурно-логическая основа которой еще очень далека от совершенства.

В соответствие с этим представляется целесообразным Министерству образования и науки Российской Федерации:

[4] Bertalanffy L. von. General System Theory: Foundations, Development, Applications. New York: George Braziller, 1968 (revised edition 1976).

[5] Большой энциклопедический словарь / Гл. ред. А. М. Прохоров. М.: БРЭ, 2002. 1456 с. ISBN 5-85270-160-2.

1) организовать работу по созданию единой и непротиворечивой классификационной системы научных специальностей, по которым присуждаются ученые степени;

2) при формировании новой редакции «Номенклатуры научных специальностей, по которым присуждаются ученые степени» осуществлять:

– безусловную реализацию требований научной классификации и систематизации исходного множества научных специальностей на предметно-ориентированные группы и подгруппы, с отдельным выделением групп *универсальных* научных специальностей;
– учет и своевременное устранение выявленных недостатков и противоречий в классификации научных специальностей;

3) в программах школьного, среднего и высшего образования предусмотреть обучение в рамках системного научного направления «Общая классификация и систематизация».

Литература

1. Богданов А.А. Тектология: (Всеобщая организационная наука). СПб., 1922. (Переиздание: в 2-х кн. М. : Экономика, 1989. 304 с. + 351 с.). ISBN 5-282-00538-7.
2. Гуссерль Э. Философия как строгая наука // Труды. Новочеркасск : Сагуна, 1994. С. 127—175.
3. Ершов В.В. Правовое и индивидуальное регулирование общественных отношений : монография. М. : РГУП, 2018. 316 с.
4. Ловцов Д.А. Системный анализ. Часть 1. Теоретические основы. М. : Рос. гос. ун-т правосудия, 2018. 224 с. ISBN 978-5-93916-701-7.
5. Ловцов Д.А. Системология научных исследований. М. : ФБУ НЦПИ при Минюсте России, 2018. 76 с. ISBN 978-5-90167-53-3.
6. Ловцов Д.А. О концепции комплексного подхода // Философские исследования. 2000. № 4. С. 158—174.
7. Ловцов Д.А. Системология правового регулирования: исторические аспекты развития // История государства и права. 2009. № 18. С. 9—12.
8. Ловцов Д.А. Системология правового регулирования информационных отношений в инфосфере. М. : Рос. гос. ун-т правосудия, 2016. 316 с. ISBN 978-5-93916-505-1.
9. Омельченко В.В. Общая теория классификации : монография. В 2 ч. Часть I. Основы системологии познания действительности (Предисл. Д.А. Ловцова) // М. : Кн. мир, 2008. 434 с. ISBN 978-5-91146-297-0.
10. Омельченко В.В. Общая теория классификации. В 2 ч. Часть II. Теоретико-множественные основания. М. : Кн. мир, 2010. 295 с. ISBN 978-5-397-01327-7.
11. Омельченко В.В. Основы систематизации. М. : Кн. дом «Либроком», 2012. 479 с. ISBN 978-5-397-02383-2.
12. Омельченко В.В. Государственное управление научной и научно-технической деятельностью в Российской Федерации на примере подготовки и принятия системы специальностей // Вестник РУДН. Сер. «Государственное и муниципальное управление». 2018. № 4. Т. 5. С. 397—410. DOI: 10.22363/2312-8313-2018-5-4-397-410 .
13. Омельченко В.В. Информационное обеспечение государственного регулирования подготовки и принятия системы научных специальностей // Правовая информатика. 2019. № 2. С. 4—14. DOI: 10.21681/1994-1404-2019-2-4-14 .
14. Омельченко В.В. Сравнительный анализ российской и международной систем классификации научных направлений (специальностей) // Правовая информатика. 2020. № 1. С. 55—63. DOI: 10.21681/1994-1404-2020-1-55-63 .
15. Системный аудит использования национальных ресурсов и управление по результатам. Вып. II. Методы и модели информационно-аналитического обеспечения / Под ред. А.А. Пискунова. Ростов-на-Дону : ЮФУ, 2007. 592 с.
16. Chomsky N. Syntactic structures. Berlin, New York: De Gruyter Mouton, 2002. 115 pp.

Рецензент: ***Емелин Николай Михайлович,*** *доктор технических наук, профессор, заслуженный деятель науки и техники РСФСР, главный научный сотрудник Государственного научно-методического центра Минобрнауки РФ, г. Москва, Россия.*
E-mail: nme47@mail.ru

THE QUALITY OF SYSTEMATISATION OF SCIENTIFIC SPECIALTIES IN THE 2021 RUSSIAN NOMENCLATURE

Victor Omel'chenko, *Dr.Sc. (Technology), Professor, Meritorious Figure of Science and Technology of the Russian Federation, State Councillor of the 1st Class of the Russian Federation, Advisor to the Secretariat of the Board for Science and Technology of the AO (JSC) "VPK "NPO Mashinostroeniia", Moscow, Russian Federation.*
E-mail: omvv@yandex.ru

Keywords: *government policy, shortcomings, nomenclature, classification, control, research area, scientific specialty, systematisation, academic degrees.*

Abstract.

Purpose of the paper: assessing the quality of systematisation and classification in the new "Nomenclature of scientists' specialties in which doctoral degrees are awarded" introduced by Order No. 118 of the Ministry of Education and Science of the Russian Federation dated the 24th February 2021.

Methods used: multi-faceted analytical and expert methods of systematisation and general classification theory, structural and logical analysis.

Results obtained: an assessment of the new "Nomenclature of scientists' specialties in which doctoral degrees are awarded" was carried out from a systemic standpoint in terms of meeting the basic requirements for the classification and systematisation of objects, processes or phenomena of reality, including a structural and logical analysis of the main changes, an assessment of the quality of the main classification schemes of the new Nomenclature as well as a semantic analysis of the systematisation of the proposed scientists' specialties. A positive dynamic was noted in eliminating a number of shortcomings, contradictions and other anomalies (inadequacies) identified in 2018-2020 in the previous "Nomenclature of scientists' specialties in which doctoral degrees are awarded" valid until the 24th February 2021. The main shortcomings of the new Nomenclature are considered and recommendations for their elimination are given.

References

1. Bogdanov A.A. Tektologiia: (Vseobshchaia organizatsionnaia nauka). SPb., 1922. (Pereizdanie: v 2-kh kn. M. : Ekonomika, 1989. 304 pp. + 351 pp.). ISBN 5-282-00538-7.
2. Gusserl' E. Filosofiia kak strogaia nauka. Trudy. Novocherkassk : Saguna, 1994, pp. 127-175.
3. Ershov V.V. Pravovoe i individual'noe regulirovanie obshchestvennykh otnoshenii : monografiia. M. : RGUP, 2018. 316 pp.
4. Lovtsov D.A. Sistemnyi analiz. Chast' 1. Teoreticheskie osnovy. M. : Ros. gos. un-t pravosudiia, 2018. 224 pp. ISBN 978-5-93916-701-7.
5. Lovtsov D.A. Sistemologiia nauchnykh issledovanii. M. : FBU NTsPI pri Miniuste Rossii, 2018. 76 pp. ISBN 978-5-90167-53-3.
6. Lovtsov D.A. O kontseptsii kompleksnogo podkhoda. Filosofskie issledovaniia, 2000, No. 4, pp. 158-174.
7. Lovtsov D.A. Sistemologiia pravovogo regulirovaniia: istoricheskie aspekty razvitiia. Istoriia gosudarstva i prava, 2009, No. 18, pp. 9-12.
8. Lovtsov D.A. Sistemologiia pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere. M. : Ros. gos. un-t pravosudiia, 2016. 316 pp. ISBN 978-5-93916-505-1.
9. Omel'chenko V.V. Obshchaia teoriia klassifikatsii : monografiia. V 2 ch. Chast' I. Osnovy sistemologii poznaniia deistvitel'nosti (Predisl. D.A. Lovtsova). M. : Kn. mir, 2008. 434 pp. ISBN 978-5-91146-297-0.
10. Omel'chenko V.V. Obshchaia teoriia klassifikatsii. V 2 ch. Chast' II. Teoretiko-mnozhestvennye osnovaniia. M. : Kn. mir, 2010. 295 pp. ISBN 978-5-397-01327-7.
11. Omel'chenko V.V. Osnovy sistematizatsii. M. : Kn. dom "Librokom", 2012. 479 pp. ISBN 978-5-397-02383-2.
12. Omel'chenko V.V. Gosudarstvennoe upravlenie nauchnoi i nauchno-tekhnicheskoi deiatel'nost'iu v Rossiiskoi Federatsii na primere podgotovki i priniatiia sistemy spetsial'nostei. Vestnik RUDN, ser. "Gosudarstvennoe i munitsipal'noe upravlenie", 2018, No. 4, t. 5, pp. 397-410. DOI: 10.22363/2312-8313-2018-5-4-397-410 .
13. Omel'chenko V.V. Informatsionnoe obespechenie gosudarstvennogo regulirovaniia podgotovki i priniatiia sistemy nauchnykh spetsial'nostei. Pravovaia informatika, 2019, No. 2, pp. 4-14. DOI: 10.21681/1994-1404-2019-2-4-14 .
14. Omel'chenko V.V. Sravnitel'nyi analiz rossiiskoi i mezhdunarodnoi sistem klassifikatsii nauchnykh napravlenii (spetsial'nostei). Pravovaia informatika, 2020, No. 1, pp. 55-63. DOI: 10.21681/1994-1404-2020-1-55-63 .
15. Sistemnyi audit ispol'zovaniia natsional'nykh resursov i upravlenie po rezul'tatam. Vyp. II. Metody i modeli informatsionno-analiticheskogo obespecheniia. Pod red. A.A. Piskunova. Rostov-na-Donu : IuFU, 2007. 592 pp.
16. Chomsky N. Syntactic structures. Berlin, New York: De Gruyter Mouton, 2002. 115 pp.

ИНТЕЛЛЕКТУАЛЬНЫЕ ПРОГРАММНО-АППАРАТНЫЕ РЕШЕНИЯ ДЛЯ АВТОМАТИЗИРОВАННЫХ ОПТИКО-ЭЛЕКТРОННЫХ СИСТЕМ РЕАЛЬНОГО ВРЕМЕНИ

Гаврилов Д.А.*

***Ключевые слова**: автоматизированные оптико-электронные системы, переработка визуальной информации, эффективность, робототехнические комплексы, техническое зрение, автоматизированная разметка, обнаружение, селекция, классификация, сопровождение целей, наземно-космический мониторинг.*

Аннотация.

Цель работы: анализ основных подходов к созданию программно-аппаратного обеспечения автоматизированных оптико-электронных систем наземно-космического мониторинга, предназначенных для решения задач сбора, обработки и хранения визуальной информации в робототехнических комплексах специального назначения с повышенной степенью автономности.

Методы исследования: экспертный анализ основных направлений и тенденций развития в области цифровых средств автоматизированной обработки визуальной информации, выработка обоснованных организационно-технических требований к информационно-техническому и программному обеспечению процессов переработки информации, анализ возможностей применения аппаратного, алгоритмического и программного обеспечения автоматизированных оптико-электронных систем в робототехнических комплексах специального назначения.

Результаты: представлены возможные перспективные направления применения аппаратного, алгоритмического и программного обеспечения систем технического зрения в робототехнических комплексах специального назначения, выделены основные направления и тенденции развития в области цифровых средств автоматизированной обработки визуальной информации. Представлены основные авторские разработки в области современных интеллектуальных систем технического зрения, основанных на автоматизированных оптико-электронных робототехнических комплексах специального назначения.

DOI: 10.21681/1994-1404-2021-3-14-24

Введение

В современных условиях определяющим фактором достижения стратегического и оперативно-тактического превосходства над противником становится поддержание высокого уровня *информационного обеспечения* [10] как для систем управления движением при решении навигационных задач, так и для систем управления вооружением при решении огневых задач. Необходимость решения задач автономного движения, навигации и управления вооружением в условиях отсутствия спутниковых навигационных сигналов требует использования перспективных средств аппаратного, алгоритмического и программного обеспечения, основанных на использовании методов искусственного интеллекта для максимально быстрого реагирования на изменяющуюся оперативную обстановку. *Требования* по обеспечению повышенной степени автономности робототехнических комплексов специального назначения оказывают непосредственное влияние на необходимость оснащения специальных служб и армии современными автоматизированными системами вооружений, средствами разведки и навигации, подвижной и роботизированной техникой различного назначения, беспилотными летательными аппаратами, функционирующими как в автономном, так и в дистанционно пилотируемом режимах [14, 17].

Задачи оперативной переработки информации, стоящие перед робототехническим комплексами специального назначения, как правило, требуют решения в режиме реального времени, поэтому все более востребованными становятся системы, использующие техническое зрение в качестве основного источника информации, получаемой при обработке изображений и разнообразных сигналов, в том числе радиолокационных. Системы технического зрения востребованы в средствах противовоздушной обороны, поисково-спасательных операциях, медицине, беспилотных и

* ***Гаврилов Дмитрий Александрович,*** *кандидат технических наук, докторант Института точной механики и вычислительной техники им. С. А. Лебедева Российской академии наук, г. Москва, Российская Федерация.*

E-mail: gavrilov.da@mipt.ru

дистанционно пилотируемых аппаратах, обеспечивающих получение, переработку и передачу визуальной информации на пункт дистанционного управления в реальном масштабе времени.

В настоящей работе рассматриваются основные подходы к созданию программно-аппаратного обеспечения автоматизированных оптико-электронных систем (АОЭС) наземно-космического мониторинга (НКМ), предназначенных для решения задач сбора, обработки и хранения визуальной информации в робототехнических комплексах специального назначения с повышенной степенью автономности.

Основные направления и тенденции развития в области цифровых средств автоматизированной обработки визуальной информации

Системы технического зрения являются одним из важнейших направлений развития автоматизированной обработки изображений. Перед разработчиками систем такого типа остро встают проблемы преобразования визуальной информации неаналитического характера в аналитические данные, в том числе в режиме реального времени в условиях высоких скоростей движения мобильных объектов сложной формы в различных фоноцелевых обстановках. На основе полученной информации оператор может сформировать план дальнейшего использования выявленных аналитических данных.

Одним из основных требований к оптико-электронной робототехнической системе является способность автономно, без участия оператора выделять во входном видеопотоке объекты интереса и осуществлять слежение за данными объектами. При этом обработка информации, получаемой оптико-электронной системой, должна осуществляться в автоматическом режиме. Оптико-электронная система приобретает роль «органов зрения», ключевым моментом построения которых является необходимость реализации качественного алгоритма обнаружения объектов [5, 7]. Современные цифровые средства формирования изображений охватывают практически весь электромагнитный спектр от гамма-излучения до радиоволн [4]. Полученные изображения позволяют проводить неограниченное число операций и процедур по их обработке, существенно отличающихся как по сложности выполнения, так и по реализации. Процесс переработки визуальной информации охватывает широкий спектр методов, имеющих различное применение. Из множества методов выделяется определенный их набор с целью построения алгоритмов для решения конкретных поставленных задач [18, 22]. Основной целью данных операций является получение информации описательного характера, позволяющей производить расширенный логический анализ имеющихся графических данных.

Таким образом, общей современной тенденцией развития систем технического зрения является совершенствование методов и средств формирования и обработки зрительной информации.

Основная функциональность систем технического зрения робототехнических комплексов специального назначения

Основную функциональность систем технического зрения робототехнических комплексов специального назначения составляет решение задач детектирования, локализации и классификации объектов на фото- и видеоданных применительно к различным фоноцелевым обстановкам. Основные трудности при решении данных задач возникают вследствие: потери информации при проецировании трехмерной сцены на плоскость изображения; наличия шума на изображении; изменения экспозиции сцены; сложной формы объектов; изменения формы объекта; частичных или полных перекрытий и загораживаний объектов сцены; сложной траектории движения объекта; выхода объекта за пределы кадра и появления объекта в кадре; относительного движения камеры; требований обработки в реальном времени [14].

Для решения каждой из задач технического зрения, как правило, требуется разработка оптимальных (подходящих) для данного типа задачи методов и алгоритмов [20, 21]. Продуктивная классификация методов переработки визуальной оптико-электронной информации включает глобальные, локальные и точечные методы (*рис*. 1).

Каждый из методов переработки включает совокупность способов обработки изображений. В свою очередь, для реализации какого-либо способа могут быть использованы разнообразные алгоритмы или инструменты. Для разных целей могут использоваться различные способы обработки или их комбинации. Чем выше сложность задачи обработки изображения, тем большее число процессов может требоваться для ее решения. При этом обработка и анализ изображений — это пошаговая процедура, зависящая от результатов предыдущего этапа. Основной стратегией является разделение сложной задачи обработки на последовательность подзадач, большинство которых решается путем применения к изображению определенного набора типовых операций обработки. Тем не менее универсальные способы и алгоритмы решения любых задач обнаружения, локализации и классификации пока не найдены.

Необходимость автоматизации дешифровки аэрокосмических изображений связана, прежде всего, со взрывным ростом объема данных дистанционного зондирования Земли и невозможностью пропорционального увеличения количества квалифицированных экспертов для их анализа. *Традиционным* подходом для решения задачи обнаружения и распознавания является использование *методов машинного обучения* с учителем. Для успешной реализации методов машинного обучения с учителем требуется накопление колоссаль-

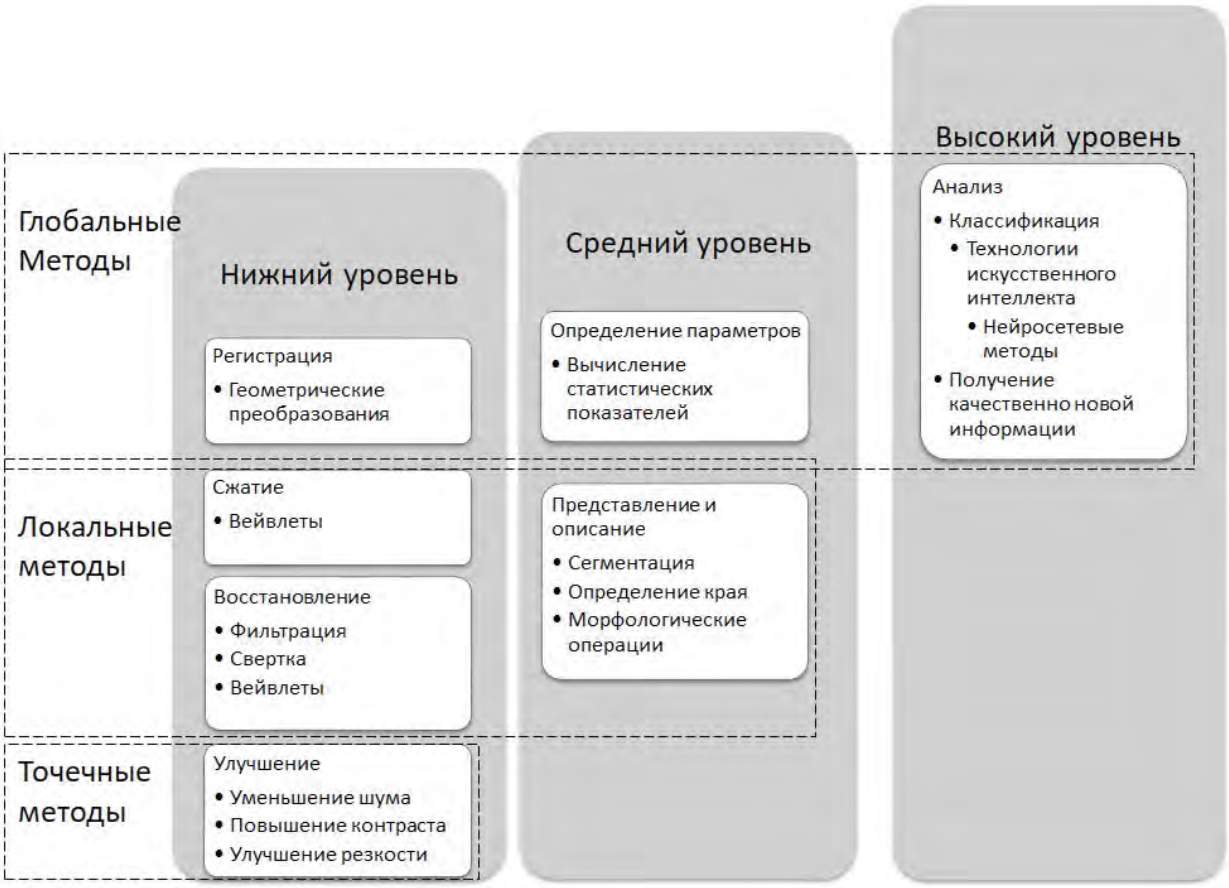

Рис. 1. Продуктивная классификация методов обработки изображений

ных объемов размеченных экспертом обучающих выборок по каждому типу объекта, в этой связи такие методы неэффективны для решения задачи обнаружения редких объектов, по которым невозможно накопить достаточную выборку; объектов, имеющих большую вариативность внешнего вида, а также скрытых объектов. Методы обучения без учителя направлены на самостоятельный поиск нейронной сетью необходимых шаблонов, корреляции в данных, извлечение *полезных признаков* непосредственно из исследуемых образцов и их анализ. Таким образом, применение методов обучения без учителя открывает возможность обработки несопоставимо бóльших объемов данных по сравнению с другими методами, поскольку не требуется ручная разметка для обучения алгоритма.

Обоснование организационно-технических требований к информационно-математическому обеспечению

АОЭС переработки визуальной информации могут быть использованы в космических системах дистанционного зондирования Земли на базе космических аппаратов (КА) «Аркон», «Канопус», «Ресурс» [9] различных модификаций и других для решения задач информационного обеспечения государственных органов управления и контроля по оперативному освещению обстановки в районах катастроф природного и техногенного характера, а также для мониторинга районов локальных конфликтов, крупных террористических актов, в качестве оптических датчиков для автоматических космических аппаратов программы исследования Луны [8].

Основная сложность при создании дистанционно пилотируемых аппаратов (ДПА) специального назначения заключается в создании необходимой для их применения системы управления, включая алгоритмы, информационные датчики, оптико-электронные системы [14, 15]. Особое место в данном случае занимает *проблема* замещения пилота как оператора управления на борту ДПА [1]. На различных этапах полета могут возникать ситуации, требующие наличия на борту ДПА полностью автономной системы управления и соответствующего информационного обеспечения.

Эффективность системы управления современных автономных ДПА в значительной мере определяется эффективностью работы алгоритмов оптико-электронной системы. Существующие оптико-электронные системы НКМ, использующие в своей работе автоматизированные методы переработки информации, часто недостаточно эффективны в отношении *точности* и *оперативности* при решении вопросов переработки визуальной информации. Основной причиной недостаточной эффективности является отсутствие фор-

мально-логического аппарата теории детектирования, локализации и классификации, обеспечивающего как выработку обоснованных требований к информационно-техническому и программному обеспечению процессов переработки информации, так и количественную оценку их эффективности и качества.

Основными организационно-техническими требованиями (ОТТ) информационно-математического обеспечения (ИМО) АОЭС НКМ, влияющими на эффективность ее функционирования, являются *точность*, характеризующая качество дешифровки визуальной информации, и *оперативность*, характеризующая обеспечение необходимого быстродействия своевременно в соответствии с поставленными целями и задачами.

Дополнительными ОТТ к ИМО АОЭС НКМ являются *имитостойкость*, характеризующая способность не допускать навязывания дезинформации в условиях информационного соперничества; *устойчивость*, характеризующая способность сохранять состояние динамического равновесия в условиях дестабилизирующих воздействий; *живучесть*, характеризующая способность выполнять установленный минимальный объем функций при подавляющих внешних воздействиях; а также *добротность*, характеризующая возможность функционирования в условиях отказов [23].

Показатели информационно-целевой эффективности [12, 13, 16] могут быть охарактеризованы следующим образом:

Информационная точность:

$$J_{1ц} = \frac{Э_ц}{\tau},$$

где

$$Э_ц = max|I_z(M,T)| = max\sum_{m=1}^{M}\left|ln\left[T(O_m)/_T\right]\right|;$$

$I_z(M,T)$ — количество получаемой от подсистемы наблюдения осведомляющей содержательной информации; O_m — оператор преобразования тезауруса T, соответствующий единичному информационному массиву (ИМ) $m \in M$; τ — средний интервал времени переработки осведомляющей информации от одного объекта управления.

Информационная добротность:

$$J_{3ц} = \frac{I}{\left[I_S + I_z[T]\right]} =$$
$$= [Э_ц + I_0 + I_V + I_z(T)]\ /[I_V + I_z(T)] =$$
$$= 1 + [Э_ц + I_0]\ /[I_V + I_z(T)].$$

где I — общее количество информации, которое хранится и циркулирует в эргасистеме (узле); I_0 — количество информации, хранимой в информационной базе эргасистемы (узла).

Информационная оперативность:

$$J_{2ц} = \frac{I}{Э_ц},$$

Информационно-технологическая эффективность характеризуется следующими показателями:

Информационная устойчивость:

$$J_{1Т} = \frac{Э_Т}{[Э_Т + I_S(\theta)]},\ J_{1Т} \in (0,1),$$

где $Э_Т = H(M_1) - \sum_i p(m_{0i})H(M_1|m_{oi})$ — мера (оценка) технологического эффекта, получаемого от данного информационного узла в результате выполнения процесса переработки информационных массивов (ИМ) m_{0i}, $i = \overline{1,M_0}$; $H(M_1) = \sum_j p(m_{1j}) \ln p(m_{1j})$ — статистическая энтропия множества переработанных ИМ; $H(M_1|m_{oi}) = \sum_j p(m_{1i}|m_{oi}) \ln p(m_{1i}|m_{oi})$ — частная (при m_{0i}) условная энтропия множества переработанных ИМ; $I_S(\theta)$ — количество используемой структурной информации, содержащейся в информационном узле, определяющее затраты на преобразование содержательной информации.

Информационная живучесть:

$$J_{2Т} = \frac{Э_Т}{N},$$

где N — сумарная производительность всех функциональных компонентов.

Информационная имитостойкость:

$$J_{3Т} = \frac{S_{ед}}{S_{общ}},$$

где $S_{ед}$ — единичное подпространство параметров; $S_{общ}$ — общее число возможных состояний системы.

Возможности применения аппаратного, алгоритмического и программного обеспечения АОЭС в робототехнических комплексах специального назначения

Обеспечение функционирования современных робототехнических комплексов требует разработки и изготовления всего тракта системы технического зрения, включая следующие основные *направления*: применение камеры видимого, *MWIR* и *LWIR* диапазонов; автоматическое детектирование (селекция), локализация, классификация объектов; сопровождение объектов (в том числе в многоспектральных системах); аппаратура (специализированные вычислители) для систем технического зрения реального времени, в том числе искусственные нейронные сети; автоматизированная разработка нейросетевых алго-

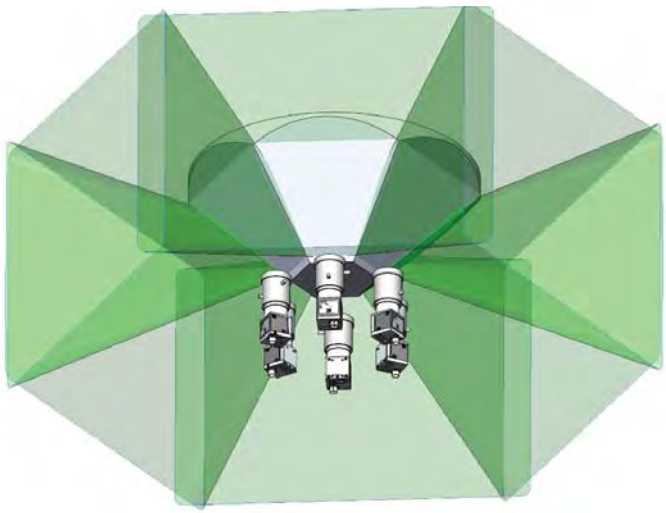

Рис. 2. Схема камеры панорамного видения

ритмов; синтезированное зрение-комплексирование изображений различных спектральных диапазонов, построение панорамных изображений; оценка *ego-motion*, стабилизация изображения [2]; многоканальные системы регистрации видеоизображения; сжатие и передача *HD*-видео по радиоканалу (90 *Мбит/с*). Основные аппаратно-программные компоненты АОЭС включают следующие.

Камера панорамного видения. В качестве основы для камеры панорамного видения разработана оптическая схема, позволяющая осуществлять панорамную съемку из одной точки (*рис*. 2). Используется 8 сенсоров. В разработке находится оптическая схема, при которой число сенсоров будет минимизировано с 8 до 6.

Данное решение позволяет обеспечивать построение панорамного изображения и поддерживать ситуационную информированность (осведомленность), а также решать задачи компьютерного зрения с применением полученного панорамного изображения. Внешний вид камеры панорамного видения представлен на рис. 3.

Портативный комплекс обнаружения, селекции, классификации и сопровождения целей. Портативный программно-аппаратный комплекс (далее — ПАК обнаружения) реализован на нейросетевой аппаратной

Рис. 3. Внешний вид камеры панорамного видения

платформе. Существует также реализация на ПЛИС. Внешний вид ПАК обнаружения представлен на *рис*. 4.

Особенностью предлагаемого ПАК обнаружения является высокая вычислительная мощность — не менее 1 *Тфлопс* при достаточно низком энергопотреблении, малых габаритных размерах и массе, которая составляет от 80 до 200 *г* в зависимости от требований по питанию и радиатору (*таблица* 1). Данные параметры обеспечены высокой энергоэффективностью нейросетевых вычислителей, а также высокой эффективностью авторских алгоритмов.

ПАК обнаружения способен обрабатывать поток видеоданных с разрешением 640×480 и частотой 30 кадров в секунду в режиме реального времени. Образцы обработанных изображений представлены на *рис*. 5.

Набор инструментов для автоматизированной разработки нейросетевых алгоритмов [3].

Программное обеспечение разметки обучающей выборки фото- и видеоданных для формирования об-

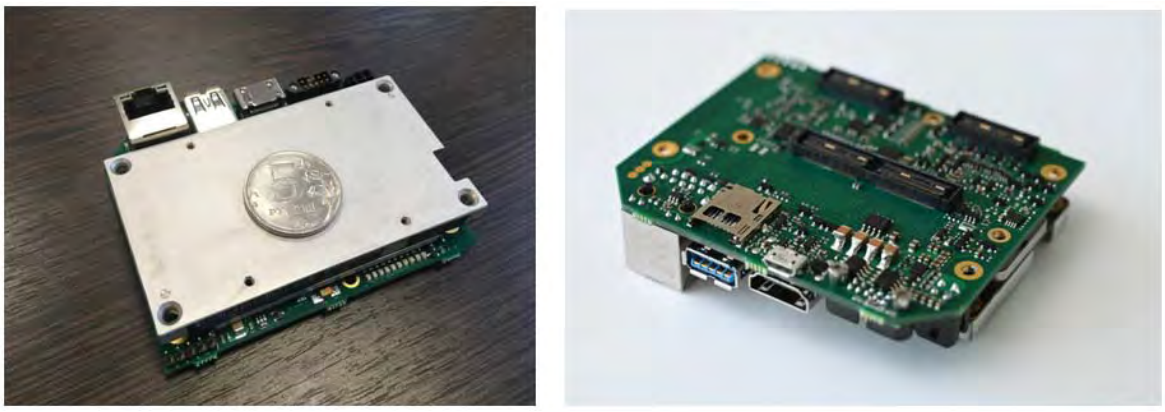

Рис. 4. Внешний вид ПАК обнаружения

Таблица 1

Технические характеристики ПАК обнаружения

Характеристика	Значение
Формат видео	произвольный не менее 50 мегапикселей в секунду, типично 1024×768×24 *бит* @ 50 *Гц*, 640×512×16 *бит* @100 Гц
Видео входы	2× *CameraLink base, Gigabit Ethernet*, *USB* 3.0, *PCIe*, *CSI* 2.0
Энергопотребление	15 *Вт*
Габариты	90×50×20 *мм*
Масса	80—200 *г*

учающих выборок позволяет проводить автоматическую подготовку исходных данных для обучения нейронной сети при решении задачи сегментации объектов интереса с целью классификации объектов по их форме [6]. Прецедентная информация для обучения представляет собой аэрокосмические снимки с отмеченными на них изображениями объектов, которые выделены оператором с максимальной возможной точностью. Внешний вид интерфейса программы разметки изображений представлен на *рис*. 6.

Применение программного обеспечения разметки обеспечивает снижение трудозатрат оператора на подготовку исходных данных для обучения нейронной сети [20]. Высокая скорость разметки достигается за счет использования асессором векторных шаблонов, описывающих границы объектов интереса, а также инструментов для подгонки шаблонов к изображениям объектов. Пример процесса разметки объектов авиационной техники представлен на *рис*. 7.

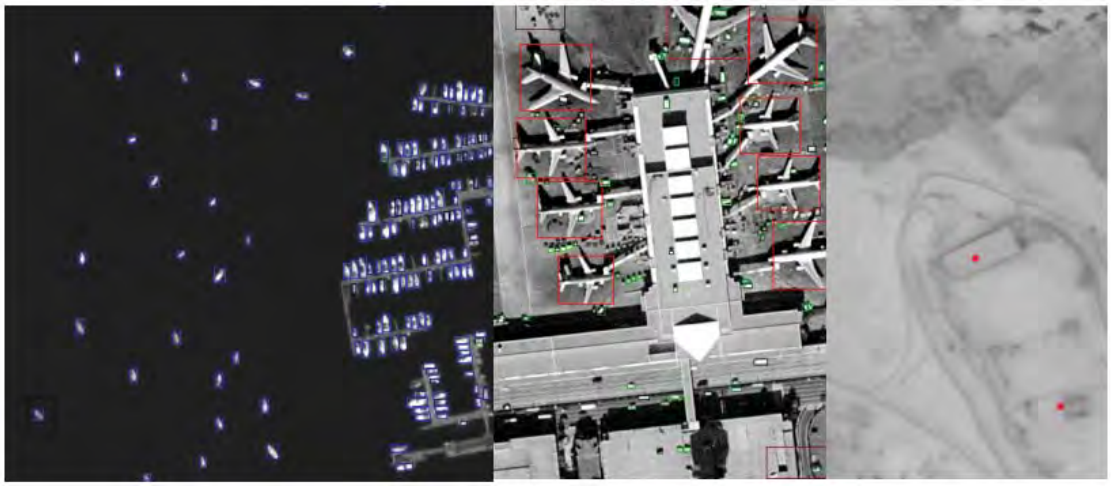

Рис. 5. Образцы обработанных изображений

Фотореалистичный симулятор видимого и инфракрасного диапазонов позволяет получать синтетические данные для пополнения и расширения обучающих выборок. Образцы реального и синтезированного изображений представлены на *рис*. 8.

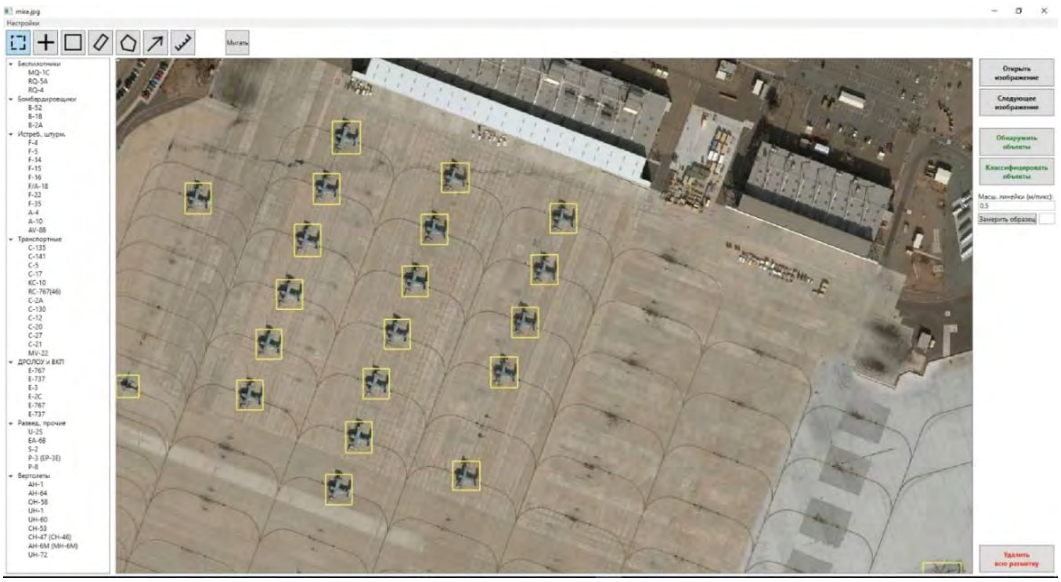

Рис. 6. Внешний вид интерфейса программы разметки изображений

Разведывательно-аналитический комплекс «Автопол»

Бортовые АОЭС широко применяются в составе разведывательно-аналитических комплексов «Автопол», включающих радиоэлектронное и алгоритмическое, интегрированное с транспортными модулями наземного или воздушного базирования различного типа обеспечение, что позволяет осуществлять оперативное наблюдение за обстановкой с воздуха и с Земли (*рис*. 9).

Комплекс включает следующие подсистемы:

– подсистема воздушного мониторинга, представляющая собой дистанционно пилотируемый (беспилотный) летательный аппарат (ДПА) [14], оснащенный оптико-электронными и тепловизионными системами наблюдения;
– подсистема наземного мониторинга, представляющая собой автомобиль с системой автоматического управления, оснащенный оптико-электронными, тепловизионными и радиолокационными системами наблюдения;
– пункт командного управления, обеспечивающий интеграцию подсистем в единый комплекс и предназначенный для сбора, анализа и визуализации воздушной и наземной обстановки.

Организация сбора и регистрации информации обеспечивается с помощью трехканальной системы сбора и регистрации фото- и видеоинформации для ДПА и робототехнических средств, технические харак-

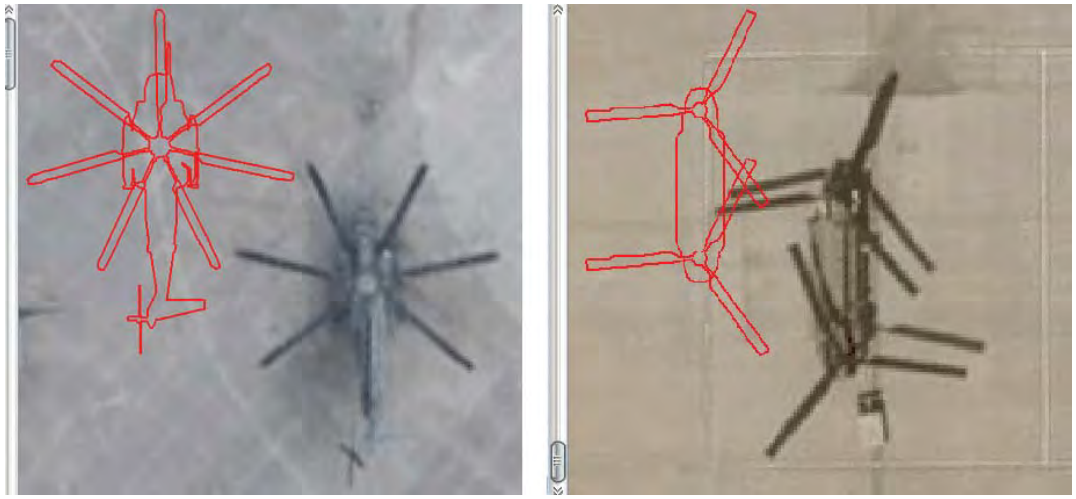

Рис. 7. Процесс разметки вертолетов

Рис. 8. Комбинирование реальных и синтезированных изображений

теристики которой представлены в *таблице* 2. Реализованные алгоритмы позволяют исследовать разновременные изображения дистанционного зондирования Земли, снятые в различных спектральных диапазонах, что обеспечивает возможность обнаружения объектов интереса как аномалий в пространственных и пространственно-временных данных [2].

Заключение

Рассмотрены основные подходы к решению задач сбора, обработки и хранения визуальной информации в робототехнических комплексах специального назначения. Необходимость автоматизации дешифровки аэрокосмических изображений связана, прежде всего, со взрывным ростом объема данных дистанционного зондирования Земли и невозможностью пропорционального увеличения количества квалифицированных экспертов для их анализа.

Выполнен анализ современного состояния и основных тенденций развития систем технического зрения, основанных на использовании методов искусственного интеллекта, показавший, что основным направлением развития в области цифровых средств автоматизированной обработки визуальной информации является совершенствование методов и средств формирования и переработки зрительной информации. Для решения каждой из задач технического зрения требуется разработка оптимальных (приемлемых) для данного типа задачи методов и алгоритмов. Обоснована продуктивная классификация методов логической обработки изображений. Обоснована совокупность основных и дополнительных организационно-технических требований к функциям, информационно-математическому и программному обеспечению АОЭС НКМ.

Рассмотрены возможности применения аппаратного, алгоритмического и программного обеспечения АОЭС в робототехнических комплексах специального назначения с учетом того, что обеспечение функционирования современных робототехнических комплексов требует разработки и изготовления всего тракта системы технического зрения.

Представлены основные аппаратно-программные компоненты АОЭС, в том числе: камера панорамного вида, позволяющая обеспечивать построение панорамного изображения и поддерживать ситуационную осведомленность, а также решать задачи компьютерного

Рис. 9. Основные компонеты разведывательно-аналитического автоматизированного комплекса «Автопол»

Таблица 2

Технические характеристики 3-канальной системы сбора и регистрации фото- и видеоинформации для ДПА и робототехнических средств

Наименование	Технические характеристики
Камера видимого диапазона	2048×1536 пикселей, 12 бит, частота кадров 100 Гц
Инфракрасная камера на базе неохлаждаемого сенсора диапазона от 8 до14 *мкм*	640×480 пикселей (в разработке 1024×768), АЦП 16 *бит*, 30 *Гц*
Инфракрасная камера на базе охлаждаемого сенсора *InSb* диапазона от 3 до 5 *мкм*	640×512, АЦП 16 б*ит*, 100 *Гц*
Габариты (без камер и гиростабилизированного подвеса)	280×195×69 *мм*
Вес (без камер и гиростабилизированного подвеса)	2,3 *кг*
Общий вес регистратора	4,9 *кг*

зрения с применением полученного панорамного изображения; портативный комплекс обнаружения, селекции, классификации и сопровождения целей, повышающий эффективность бортовых систем обработки фото- и видеоданных без необходимости сжатия, шифрования и последующей передачи на землю, что существенно сокращает время принятия решения и минимизирует риск утечки; набор инструментов для автоматизированной разработки нейросетевых алгоритмов, обеспечивающий снижение трудозатрат оператора на подготовку исходных данных для обучения нейронной сети.

Приведены общее описание и характеристики разведывательно-аналитического комплекса «Автопол», включающего совокупность алгоритмического, радиоэлектронного и вычислительного обеспечения, интегрированного с транспортными модулями наземного или воздушного базирования различного типа и позволяющего осуществлять оперативное наблюдение за обстановкой из космоса (с воздуха) и с Земли. Реализованные алгоритмы позволяют исследовать разновременные изображения дистанционного зондирования Земли, снятые в различных спектральных диапазонах, что обеспечивает возможность обнаружения объектов интереса как аномалий в пространственных и *пространственно-временных данных* [19].

Разработанные аппаратные, алгоритмические и программные решения имеют значительные перспективы для решения практических задач автономного движения, навигации и управления робототехнических комплексов специального назначения.

Литература

1. Васильев В.В., Джуган Р.В. Отождествление беспилотных летательных аппаратов в оптико-электронной системе контроля их группового полета // Правовая информатика. 2021. № 2. С. 40—48. DOI: 10.21681/1994-1404-2021-2-40-48 .
2. Гаврилов Д.А., Ивкин А.В., Щелкунов Н.Н. Система тестирования алгоритмов стабилизации видеоизображений, функционирующих в режиме реального времени // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение». 2018. № 6. С. 22—36.
3. Гаврилов Д.А., Ловцов Д.А. Автоматизированная переработка визуальной информации с помощью технологий искусственного интеллекта // РАН. Искусственный интеллект и принятие решений. 2020. № 10. С. 33—46. DOI: 10.14357/20718594200404 .
4. Гаврилов Д.А., Мелерзанов А.В., Щелкунов Н.Н., Закиров Э.И. Применение технологий глубокого обучения для диагностики кожных заболеваний на основе нейронных сетей // Медицинская техника. 2018. № 5. С. 26—39.
5. Гаврилов Д.А., Павлов А.В. Поточная аппаратная реализация алгоритма SURF // Известия ВУЗов. Электроника. 2018. Т. 23. № 5. С. 502—511.
6. Гаврилов Д.А., Щелкунов Н.Н. Программное обеспечение разметки крупноформатных аэрокосмических изображений и подготовки обучающих выборок // Научное приборостроение. 2020. Т. 30. № 2. С. 67—75.
7. Гаврилов Д.А., Павлов А.В., Щелкунов Д.Н. Аппаратная реализация сжатия динамического диапазона цифровых изображений на ПЛИС Xilinx // Журнал радиоэлектроники. 2018. № 10. URL: http://jre.cplire.ru/jre/oct18/6/text.pdf .
8. Ефанов В.В. Многофункциональная космическая платформа «Навигатор». Химки : НПО им. С. А. Лавочкина, 2017. 358 с.
9. Ефанов В.В., Клименко Н.Н., Семункина В.И. и др. Космическая система дистанционного зондирования Земли на базе космического аппарата «АРКОН»: к 20-летию первого запуска // Вестник НПО им С.А. Лавочкина. 2017. № 4. С. 25—34.

10. Ловцов Д.А. Информационная теория эргасистем : тезаурус. М. : Наука, 2005. 248 с. ISBN 5-02-033779-X.
11. Ловцов Д.А. Информационная теория эргасистем : монография. М. : Рос. гос. ун-т пр-судия, 2021. 314 с. ISBN 978-5-93916-887-8.
12. Ловцов Д.А. Эффективность правовых эргасистем в инфосфере // Правовая информатика. 2020. № 1. С. 4—14. DOI: 10.21681/1994-1404-2020-1-04-14 .
13. Ловцов Д.А. Информационные показатели эффективности функционирования АСУ сложными динамическими объектами // Автоматика и телемеханика. 1994. № 12. С. 143—150.
14. Ловцов Д.А., Гаврилов Д.А. Моделирование оптико-электронных систем дистанционно пилотируемых аппаратов : монография. М. : Технолоджи-3000, 2019. 164 с. ISBN 978-5-94472-036-8.
15. Ловцов Д.А., Гаврилов Д.А. Вопросы оперативной переработки визуальной информации в АОЭС наземно-космического мониторинга // Тр. VI Междунар. науч.-прак. конф. «Информационные технологии и нанотехнологии — ИТНТ-20» (26—29 мая 2020 г.). В 4-х т. / ИСОИ РАН, СНИУ. Т. 2. Обработка изображений и дистанционное зондирование Земли. Самара : Самарский ун-т, 2020. С. 271—276.
16. Ловцов Д.А., Гаврилов Д.А. Эффективная автоматизированная оптико-электронная система аэрокосмического мониторинга // Правовая информатика. 2019. № 2. С. 29—35. DOI: 10.21681/1994-1404-2021-2-29-35 .
17. Ловцов Д.А., Гаврилов Д.А., Татаринова Е.А. Эффективная автоматизированная переработка визуальной информации в оптико-электронной системе наземно-космического мониторинга // Профессорский журнал. Сер. «Технические науки». 2019. № 3. С. 26—40.
18. Ловцов Д.А., Князев К.В. Защищенная биометрическая идентификация в системах контроля доступа. I. Математические модели и алгоритмы // Информация и космос. 2013. № 1. С. 100—103.
19. Ловцов Д.А., Черных А.М. Геоинформационные системы. М. : Российская академия правосудия, 2012. 188 с. ISBN 978-5-93916-340-8.
20. Местецкий Л.М., Гаврилов Д.А., Семенов А.Б. Метод разметки изображений самолетов на аэрокосмических снимках на основе непрерывных морфологических моделей // Программирование. 2019. № 6. С. 3—13.
21. Омельченко В.В. Общая теория классификации. Ч. 1. Основы системологии познания действительности. М. : ИПЦ «Маска», 2008. 436 с.
22. Пунь А.Б., Гаврилов Д.А., Щелкунов Н.Н., Фортунатов А.А. Алгоритм адаптивной бинаризации объектов в видеопоследовательности в режиме реального времени // Успехи современной радиоэлектроники. 2018. № 8. С. 40—48.
23. Lovtsov D.A., Gavrilov D.A. Automated special purpose optical electronic system's functional diagnosis // Proceedings of International Seminar on Electron Devices Design and Production, SED-2019 (23—24 April 2019). Prague, Czech Republic: IEEE, 2019. Pp. 70-73.

*Рецензент: **Бурый Алексей Сергеевич**, доктор технических наук, эксперт РАН, директор департамента ФГУП «Российский научно-технический центр информации по стандартизации, метрологии и оценке соответствия», Российская Федерация, г. Москва.*
E-mail: a.s.burij@gostinfo.ru

INTELLIGENT SOFTWARE AND HARDWARE SOLUTIONS FOR AUTOMATED REAL TIME ELECTRONIC OPTICAL SYSTEMS

Dmitrii Gavrilov, *Ph.D. (Technology), postdoctoral student at the Lebedev Institute of Precision Mechanics and Computer Engineering of the Russian Academy of Sciences, Moscow, Russian Federation.*
E-mail: gavrilov.da@mipt.ru

Keywords: *automated electronic optical systems, visual information processing, efficiency, robotic complexes, technical vision, automated marking, detection, selection, classification, target tracking, ground and space monitoring.*

Abstract.

Purpose of the paper: analysing the main approaches to setting up software and hardware for automated electronic optical systems for ground and space monitoring intended to solve the tasks of collecting, processing and storing visual information in special applications robotic complexes with an increased autonomy.

Methods used: expert analysis of the main lines and development trends in the field of digital tools for automated processing of visual information, working out justified organisational and technical requirements for information technology and software support for information processing, analysis of the possibilities for using hardware, algorithms and software for automated electronic optical systems in special applications robotic complexes.

Results obtained: possible promising areas of applying hardware, algorithms and software for technical vision systems

in special applications robotic complexes are presented, the main lines and development trends in the field of digital tools for automated processing of visual information are highlighted. The author's main works in the field of modern intelligent systems of technical vision based on automated special applications electronic optical robotic complexes are presented.

References

1. Vasil'ev V.V., Dzhugan R.V. Otozhdestvlenie bespilotnykh letatel'nykh apparatov v optiko-elektronnoi sisteme kontrolia ikh gruppovogo poleta. Pravovaia informatika, 2021, No. 2, pp. 40-48. DOI: 10.21681/1994-1404-2021-2-40-48 .
2. Gavrilov D.A., Ivkin A.V., Shchelkunov N.N. Sistema testirovaniia algoritmov stabilizatsii videoizobrazhenii, funktsioniruiushchikh v rezhime real'nogo vremeni. Vestnik MGTU im. N.E. Baumana, ser. "Priborostroenie", 2018, No. 6, pp. 22-36.
3. Gavrilov D.A., Lovtsov D.A. Avtomatizirovannaia pererabotka vizual'noi informatsii s pomoshch'iu tekhnologii iskusstvennogo intellekta. RAN. Iskusstvennyi intellekt i priniatie reshenii, 2020, No. 10, pp. 33-46. DOI: 10.14357/20718594200404 .
4. Gavrilov D.A., Melerzanov A.V., Shchelkunov N.N., Zakirov E.I. Primenenie tekhnologii glubokogo obucheniia dlia diagnostiki kozhnykh zabolevanii na osnove neironnykh setei. Meditsinskaia tekhnika, 2018, No. 5, pp. 26-39.
5. Gavrilov D.A., Pavlov A.V. Potochnaia apparatnaia realizatsiia algoritma SURF. Izvestiia VUZov. Elektronika, 2018, t. 23, No. 5, pp. 502-511.
6. Gavrilov D.A., Shchelkunov N.N. Programmnoe obespechenie razmetki krupnoformatnykh aerokosmicheskikh izobrazhenii i podgotovki obuchaiushchikh vyborok. Nauchnoe priborostroenie, 2020, t. 30, No. 2, pp. 67-75.
7. Gavrilov D.A., Pavlov A. V., Shchelkunov D.N. Apparatnaia realizatsiia szhatiia dinamicheskogo diapazona tsifrovykh izobrazhenii na PLIS Xilinx. Zhurnal radioelektroniki, 2018, No. 10. URL: http://jre.cplire.ru/jre/oct18/6/text.pdf .
8. Efanov V.V. Mnogofunktsional'naia kosmicheskaia platforma "Navigator". Khimki : NPO im. S. A. Lavochkina, 2017. 358 pp.
9. Efanov V.V., Klimenko N.N., Semunkina V.I. i dr. Kosmicheskaia sistema distantsionnogo zondirovaniia Zemli na baze kosmicheskogo apparata "ARKON": k 20-letiiu pervogo zapuska. Vestnik NPO im S.A. Lavochkina, 2017, No. 4, pp. 25-34.
10. Lovtsov D.A. Informatsionnaia teoriia ergasistem : tezaurus. M. : Nauka, 2005. 248 c. ISBN 5-02-033779-Kh.
11. Lovtsov D.A. Informatsionnaia teoriia ergasistem : monografiia. M. : Ros. gos. un-t pr-sudiia, 2021. 314 pp. ISBN 978-5-93916-887-8.
12. Lovtsov D.A. Effektivnost' pravovykh ergasistem v infosfere. Pravovaia informatika, 2020, No. 1, pp. 4-14. DOI: 10.21681/1994-1404-2020-1-04-14 .
13. Lovtsov D.A. Informatsionnye pokazateli effektivnosti funktsionirovaniia ASU slozhnymi dinamicheskimi ob"ektami. Avtomatika i telemekhanika, 1994, No. 12. C. 143-150.
14. Lovtsov D.A., Gavrilov D.A. Modelirovanie optiko-elektronnykh sistem distantsionno pilotiruemykh apparatov : monografiia. M. : Tekhnolodzhi-3000, 2019. 164 pp. ISBN 978-5-94472-036-8.
15. Lovtsov D.A., Gavrilov D.A. Voprosy operativnoi pererabotki vizual'noi informatsii v AOES nazemno-kosmicheskogo monitoringa. Tr. VI Mezhdunar. nauch.-prak. konf. "Informatsionnye tekhnologii i nanotekhnologii -- ITNT-20" (26-29 maia 2020 g.), v 4-kh t., ISOI RAN, SNIU, t. 2. Obrabotka izobrazhenii i distantsionnoe zondirovanie Zemli. Samara : Samarskii un-t, 2020, pp. 271-276.
16. Lovtsov D.A., Gavrilov D.A. Effektivnaia avtomatizirovannaia optiko-elektronnaia sistema aerokosmicheskogo monitoringa. Pravovaia informatika, 2019, No. 2, pp. 29-35. DOI: 10.21681/1994-1404-2021-2-29-35 .
17. Lovtsov D.A., Gavrilov D.A., Tatarinova E.A. Effektivnaia avtomatizirovannaia pererabotka vizual'noi informatsii v optiko-elektronnoi sisteme nazemno-kosmicheskogo monitoringa. Professorskii zhurnal, ser. "Tekhnicheskie nauki", 2019, No. 3, pp. 26-40.
18. Lovtsov D.A., Kniazev K.V. Zashchishchennaia biometricheskaia identifikatsiia v sistemakh kontrolia dostupa. I. Matematicheskie modeli i algoritmy. Informatsiia i kosmos, 2013, No. 1, pp. 100-103.
19. Lovtsov D.A., Chernykh A.M. Geoinformatsionnye sistemy. M. : Rossiiskaia akademiia pravosudiia, 2012. 188 pp. ISBN 978-5-93916-340-8.
20. Mestetskii L.M., Gavrilov D.A., Semenov A.B. Metod razmetki izobrazhenii samoletov na aerokosmicheskikh snimkakh na osnove nepreryvnykh morfologicheskikh modelei. Programmirovanie, 2019, No. 6, pp. 3-13.
21. Omel'chenko V.V. Obshchaia teoriia klassifikatsii. Ch. 1. Osnovy sistemologii poznaniia deistvitel'nosti. M. : IPTs "Maska", 2008. 436 pp.
22. Pun' A.B., Gavrilov D.A., Shchelkunov N.N., Fortunatov A.A. Algoritm adaptivnoi binarizatsii ob"ektov v videoposledovatel'nosti v rezhime real'nogo vremeni. Uspekhi sovremennoi radioelektroniki, 2018, No. 8, pp. 40-48.
23. Lovtsov D.A., Gavrilov D.A. Automated special purpose optical electronic system's functional diagnosis. Proceedings of International Seminar on Electron Devices Design and Production, SED-2019 (23-24 April 2019). Prague, Czech Republic: IEEE, 2019. Pp. 70-73.

ИНФОРМАЦИОННЫЕ И ПРОГРАММНЫЕ АСПЕКТЫ РАЗРАБОТКИ И ПРИМЕНЕНИЯ СМАРТ-КОНТРАКТОВ

Федосеев С.В.*

***Ключевые слова**: байткод смарт-контракта, программные инструменты для разработки смарт-контрактов, виртуальная машина Ethereum, интегрированные среды разработки, язык программирования Solidity, оракул в блокчейн-сети, набор команд виртуальной машины Solidity, стековая организация вычислительной машины.*

Аннотация.

Цель работы: обоснование методических подходов к решению задач разработки и применения смарт-контрактов.

Методы: логическое моделирование правовых отношений и информационных связей, связанных с применением смарт-контрактов; системный анализ взаимосвязи предметной области правовой сферы, объектов сферы информационных сетевых технологий, программных средств, математических алгоритмов, основных объектов и методов теории принятия решений и теории множеств.

Результаты: выполнен анализ характеристик и методов применения программных инструментов, предназначенных для разработки, тестирования, развертывания и применения смарт-контрактов; определены характеристики, особенности использования и алгоритмические возможности языка программирования высокого уровня, предназначенного для разработки смарт-контрактов; выполнен анализ особенностей функционирования и применяемого набора операций виртуальной машины блокчейн-сети; представлена модель информационного взаимодействия постоянного хранилища, основной памяти и стека виртуальной машины блокчейн-сети; исследованы средства обеспечения информационного взаимодействия смарт-контракта с внешней средой.

DOI: 10.21681/1994-1404-2021-3-25-33

Введение. Общая характеристика смарт-контрактов

Концепция смарт-контрактов не является новой. Прототипы современных смарт-контрактов появились еще в конце 1990-х годов. Возобновление интереса к концепции смарт-контрактов связано с появлением технологии *блокчейн* и развитием средств обработки информации в сети [2, 7, 8, 12, 15].

Применяемые в сетях блокчейн программные и интерфейсные средства и языки программирования имеют высокую алгоритмическую сложность и обладают специфическими особенностями [1, 16, 17]. Анализ этих алгоритмов и особенностей представляет несомненный интерес.

Смарт-контракт — это договор между двумя и более сторонами об установлении, изменении или прекращении юридических прав и обязанностей, в котором часть или все условия записываются, исполняются и/или обеспечиваются компьютерным алгоритмом автоматически в специализированной программной среде [1, 5, 13].

Смарт-контракт может быть также определен как документ (компьютерная программа), соответствующий содержанию соглашения, которое автоматически выполняется при возникновении соответствующих условий.

Основными чертами смарт-контракта являются:

- реализация соглашения между сторонами согласно бизнес-логике;
- семантическая однозначность;
- автоматическое выполнение при достижении определенных условий;
- обеспечение правоприменения.

Вопрос правоприменения смарт-контракта является одним из важнейших [3, 10, 11, 17]. Смарт-контракт не может являться основанием для разрешения судебных споров, что связано с трудностью подтверждения соответствия «код — это закон». Однако обеспечивается следующее положение: если не возникают события, не предусмотренные условиями смарт-контракта, то отсутствует и необходимость в арбитре или третьей стороне для контроля либо влияния на его выполнение.

Если же такие события происходят, то смарт-контракт, не имеющий правил принятия решений в таких условиях, просто останавливается, прекращает свою работу.

* ***Федосеев Сергей Витальевич,*** *кандидат технических наук, доцент, профессор кафедры информационного права, информатики и математики Российского государственного университета правосудия, г. Москва, Российская Федерация.*
E-mail: fedsergvit@mail.ru

1. Рикардианские контракты

Идея представления текста заключаемого договора с использованием программного кода с последующим автоматическим его исполнением впервые была реализована в рикардианских контрактах. Эти контракты применялись в платежной системе *Ricardo* (отсюда их название) и предназначались для торговли облигациями. Первоначально рикардианские контракты реализовывались без использования технологии блокчейн.

Рикардианский контракт может быть определен как юридически обязывающий цифровой договор, определяющий условия взаимодействия двух или нескольких сторон, который криптографически [4, 9] подписан и подтвержден и читается как человеком, так и машиной[1].

Договор излагается на юридическом языке с внесением в текст меток для обеспечения машинного чтения. Обязательная *юридическая сила* основывается на предусмотренной процедуре предварительного согласования договора. Это обстоятельство, а также то, что контракт содержит условия, определенные в юридических терминах, позволяет использовать рикардианские контракты для судебного разрешения споров [18].

Следует заметить, что рикардианский контракт излагает намерения сторон, фиксирует юридическое соглашение, а также основанные на этом соглашении действия, которые предполагаются происходящими в будущем.

Наиболее часто рикардианские контракты применяются в финансовой сфере, которая характеризуется относительно простой бизнес-логикой, что делает возможным использовать простые конструкции программного кода.

Рикардианские контракты могут стать важной частью соглашений о блокчейн и заменить смарт-контракты, так как они могут одновременно действовать как смарт-контракты.

2. Инструменты для разработки смарт-контрактов

Набор программных средств, применяемых для разработки смарт-контрактов, достаточно широк. На рис.1 представлены лишь наиболее часто применяемые инструменты.

Для разработки программного кода смарт-контракта в *Ethereum* могут быть использованы два языка программирования:

- *Solidity* — наиболее популярный язык, являющийся, по сути, стандартом для рассматриваемой предметной области;
- *Vyper* — более простой язык, реже используемый, имеющий сходство с *Python*.

Другие, разработанные ранее языки программирования (такие, как *Mutan*, *LLL*, *Serpent*) в настоящее время практически не используются.

Компиляторы. Программный код, разработанный на языке высокого уровня (*Solidity* и *Vyper* являются такими языками), должен быть подвергнут компиляции для получения байткода (машинного кода), представляемого в двоичном формате.

В большинстве случаев эта процедура выполняется в *Ethereum* с использованием компилятора *Solc*. Полученный в результате компиляции байткод реализуется на виртуальной машине *Ethereum* (*EVM — Ethereum Virtual Machine*).

Основными функциями компилятора *Solc* являются:

- вывод программного кода контракта в двоичном формате;
- генерация *ABI*-интерфейса (*Application Binary Interface* — двоичный интерфейс приложений), который обеспечивает взаимодействие между байткодом (уровень виртуальной машины *EVM*) и программным кодом на языке высокого уровня;
- компиляция.

IDE (Integrated Development Environment) — интегрированные среды разработки).

Интегрированная среда *Remix* наиболее часто используется для разработки, отладки, тестирования и развертывания смарт-контрактов, написанных на языке *Solidity*.

Используется также и другая среда разработки — *Ethereum Studio*, обеспечивающая совершенный доступ к сети *Ethereum*.

API и инструменты.

API (*Application Programming Interface*) — программный интерфейс приложения. Именно посредством *API* отдельные программные компоненты взаимодействуют между собой. Компоненты могут быть низко- и высокоуровневыми, образовывать при этом сложную иерархию и использовать для взаимодействия *API* друг друга.

MetaMask — это инструмент, обеспечивающий возможность взаимодействия браузеров *Firefox* и *Chrome* с блокчейном *Ethereum* и позволяющий производить проверку транзакций, управлять учетными записями.

Личный блокчейн для тестирования.

Проверка программного кода разработанного смарт-контракта может быть выполнена в тестовой сети или в специально настроенной частной сети. Однако наиболее удобным для такой проверки программным средством является эмулятор *TestRPC*, значительно ускоряющий процедуру тестирования.

Ganache — инструмент, выполняющий те же функции, что и эмулятор *TestRPC*, но имеющий более совершенный пользовательский интерфейс и позволяющий получать подробную информацию о блоках и транзакциях.

Фреймворки.

Это программное обеспечение (платформа), облегчающее разработку и объединение разных компонентов большого программного проекта.

Truffle — среда разработки, которая с успехом применяется в *Ethereum* для тестирования и развертывания смарт-контрактов в любой сети этого блокчейна: тестовой, частной, публичной.

[1] *См.*: URL: https://iang.org/papers/fc7.html .

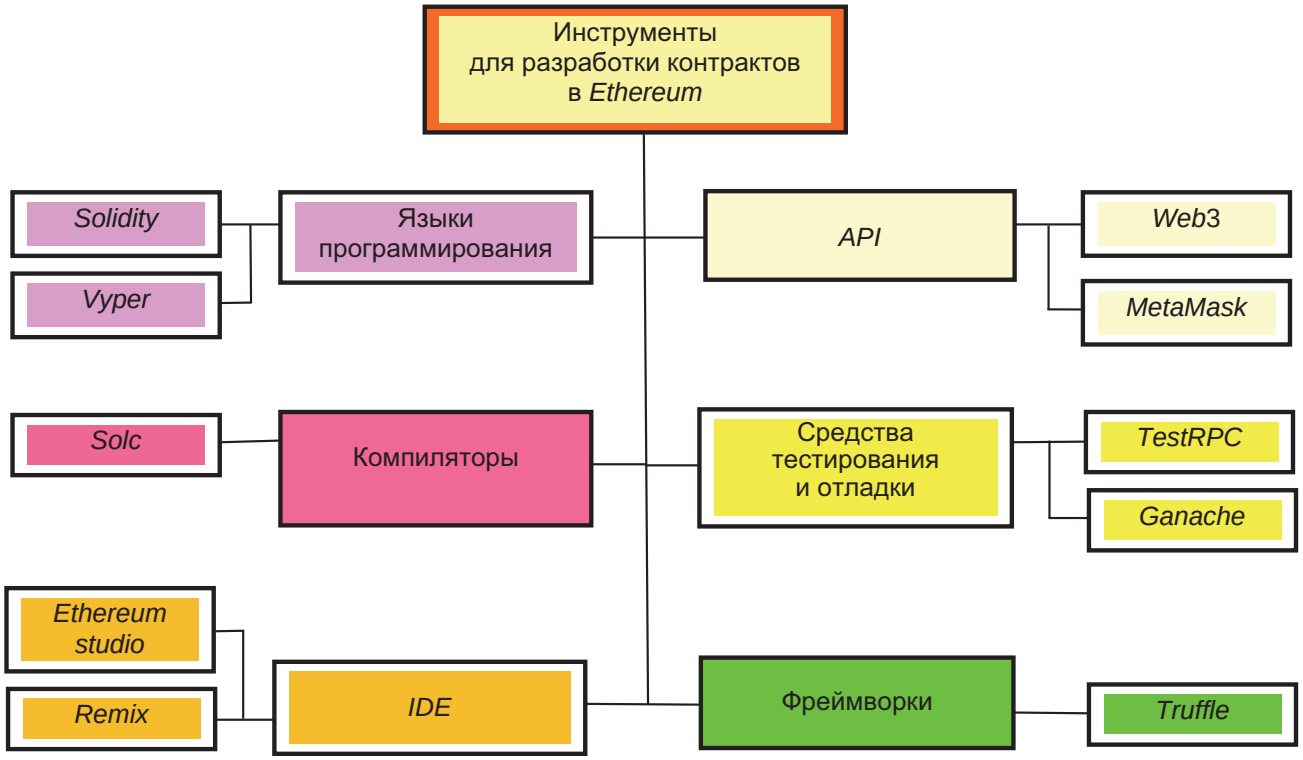

Рис. 1. Программные средства разработки контрактов в Ethereum

3. Язык программирования *Solidity*

Solidity определяется как объектно-ориентированный, предметно-ориентированный язык программирования, применяемый при разработке самовыполняющихся контрактов (смарт-контрактов) для блокчейн-платформы *Ethereum*.

Синтаксис языка *Solidity* подобен синтаксису языков *Java* и *C*. Этот язык успешно применяется для написания программных кодов смарт-контрактов. Однако по своим возможностям, по соответствию стандартам объектно-ориентированного программирования он уступает таким развитым языкам, как *Java*, *C++*, *C#*.

Особенностями языка *Solidity* являются динамические типы возвращаемых значений и статическая типизация переменных. Последнее означает, что любая переменная (локальная или глобальная) обязательно должна иметь тип, который указывается явно. Это позволяет на этапе компиляции выявлять ошибки, связанные с интерпретацией типов данных.

Реализация базовых принципов объектно-ориентированного программирования (наследование, инкапсуляция, полиморфизм) также имеет ряд особенностей.

Так, функциональностью класса (базовой сущности традиционного объектно-ориентированного языка) в *Solidity* наделяется контракт. И именно между контрактами осуществляется *наследование*, в результате которого переменные и функции наследуемого контракта сохранятся в точном соответствии в наследующем контракте и будут в нем доступны для использования. В связи с этим *Solidity* иногда определяют как контрактно-ориентированный язык.

В *Solidity* используются две категории типов данных: примитивные (простые) и ссылочные. Различие между ними состоит в том, что при выполнении операции присваивания или при передаче в функцию в качестве параметра использование данных первой категории приводит к передаче самого значения, а при использовании данных ссылочного типа — ссылки на то место памяти, где располагается используемое значение.

Основные типы данных.

Логический (булевый тип) — *bool*. Данные этого типа могут принимать два возможных значения: *true* и *false*.

Целые числа — этот тип данных может представлять целые знаковые *(int)* или целые беззнаковые числа (*uint*).

Адресный тип (*address*) — данные этого типа имеют значность 160 *бит* и состоят из нескольких полей, каждое из которых имеет свое предназначение при направлении запросов к контрактам и организации взаимодействия с ними.

Если на месте названия типа указано ключевое слово *var*, то выполняется автоматическое определение типа, при этом компилятор устанавливает переменной тип по значению, которое этой переменной присваивается.

Локальные переменные (типа *memory*) используются только при выполнении функции, с которой они связаны, и стираются по завершении этой функции.

Переменные состояния контракта (типа *storage*) связаны уже не с функцией, а с самим контрактом. Они определяют свойства контракта аналогично свойствам класса в объектно-ориентированном программировании.

Литералы в языке *Solidity* могут быть следующих видов: целочисленные литералы (последовательности десятичных цифр); строковые литералы (последовательность символов); шестнадцатеричные литералы.

Массивы в *Solidity*, так же как и в других языках программирования, определяются как набор смежных однотипных элементов, расположенных по определенному адресу в памяти. Отдельный элемент массива адресуется по значению его индекса.

С массивами в языке *Solidity* связаны два метода: *push* — добавляет новый элемент в массив; *length* — позволяет определить количество элементов в массиве.

Структуры в *Solidity* представляют собой конструкции, позволяющие объединять в единую логическую группу разнотипные данные.

Ключевое слово *struct* используется для объявления переменной структурного типа. Доступ к элементам структуры осуществляется с использованием оператора доступа — точки между объявленным именем структуры и именем адресуемого элемента.

Управляющие конструкции представлены в *Solidity* следующим набором средств разработки программного кода: *if…else; do; while; for; break; continue; return*. Эти управляющие конструкции используются так же, как и в других языках программирования (*JavaScript* или *C*).

Функции в *Solidity* связаны с контрактом. Они, как обычно, представляют собой модуль, который состоит из набора команд и многократно используется в процессе вычислений.

Для объявления функции используется ключевое слово *function*. Далее указываются: уникальное имя функции, набор параметров (может быть пустым), спецификаторы видимости (модификаторы доступа), ключевое слово *constant* (может отсутствовать), тип возвращаемого значения.

Ключевое слово *constant* определяет невозможность изменения функцией значений переменных в контракте. Она может использовать эти значения только для выполнения вычислений.

Если вызов функции выполняется из пределов рассматриваемого контракта, то такой вызов называется *внутренним*. Вызов называется *внешним*, если происходит обращение к функции, расположенной в другом контракте.

В *Solidity* при объявлении функций используются следующие спецификаторы видимости (модификаторы доступа):

external — функции этого типа могут быть вызваны из других контрактов и транзакций; стандартные процедуры не позволяют вызвать *external*-функцию внутри контракта, однако использование ключевого слова *this* позволяет это сделать;

internal — функции этого типа используются для обеспечения наследования в языке *Solidity*; такая функция, являясь внутренней функцией контракта-родителя, становится доступной дочерним контрактам;

public — функции типа *public* доступны как извне (из других контрактов и транзакций), так и изнутри контракта, они могут быть вызваны;

private — функции типа *private* отличаются от *internal* тем, что они недоступны для вызова из наследуемых дочерних контрактов и могут быть вызваны только из того контракта, где были объявлены.

Язык *Solidity* является представителем предметно-ориентированных языков (*DSL — Domain Specific Languages*). Это языки программирования, которые отражают специфику определенной предметной области, используют особые понятия и правила. По сравнению с универсальными языками программирования (*GPL — General-purpose Programming Languages*) они имеют меньший набор функций, который приспособлен для решения задач этой предметной области.

Приведем в качестве примера список доменных языков, используемых для разработки смарт-контрактов в финансовой сфере:

AxLang — DSL для написания проверяемых смарт-контрактов *Ethereum*;

Hyperledger Composer — среда разработки с открытым исходным кодом и *DSL* для написания смарт-контрактов в блокчейне *Hyperledger*;

Imandra — набор языков и инструментов для моделирования и проверки свойств финансовых бирж и смарт-контрактов *Ethereum*;

KolibriFX — язык для определения торговых стратегий иностранной валюты (*FX*) для исполнения на их облачной торговой платформе;

Marlowe — язык, ориентированный на финансовые контракты на блокчейнах;

Pyramid — DSL для написания смарт-контрактов для виртуальной машины *Ethereum*;

Rholang — язык смарт-контрактов, разработанный для технологии блокчейн *Synereo*, *RChain*.

4. Виртуальная машина *Ethereum* (*EVM*)

Виртуальная машина *Ethereum* представляет собой стековую среду, которая играет определяющую роль при реализации смарт-контрактов.

На этой виртуальной машине выполняется байткод контракта, полученный компилированием (переводом на машинный язык) исходного кода контракта, представленного на языке высокого уровня.

Машина *EVM* реализована в виде программы, экземпляр которой находится на любом узле сети *Ethereum*, имеющем полную функциональность. Она является тьюринг-полным автоматом, т. е. обладает полным набором инструкций (команд) для выполнения сложных алгоритмов обработки данных. В настоящее время *EVM* располагает набором из приблизительно 140 команд.

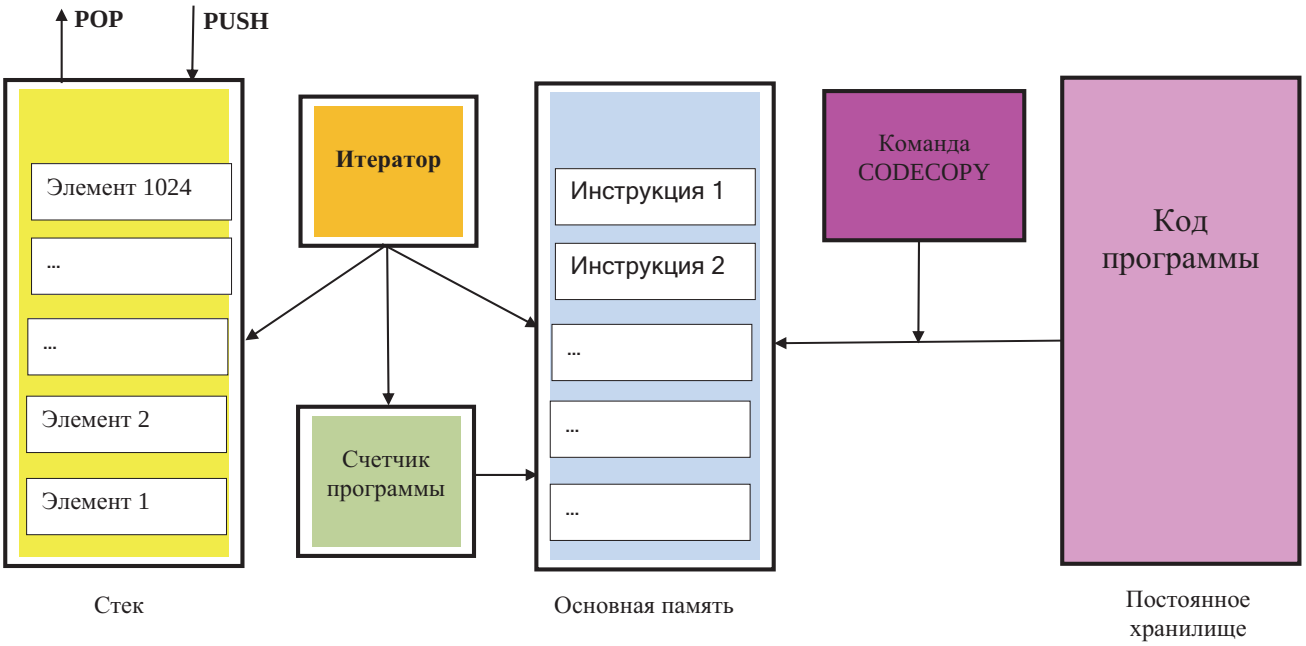

Рис. 2. Информационное взаимодействие постоянного хранилища, основной памяти и стека

Инструкции из этого набора обеспечивают выполнение процедур, разных по вычислительной сложности, которая измеряется специальной единицей вычислительной работы — *газ* (*gas*).

Выделяют два варианта платы за *газ*:

– фиксированный расход газа (*газ*, затраченный при выполнении команд, например, арифметических);
– динамически регулируемый расход газа (например, за размещение операндов и команд во всех местах хранения, кроме стека).

Суммирование вычислительных сложностей всех инструкций, составляющих байткод конкретного контракта, позволяет определить объем вычислительной работы, необходимой для его выполнения.

За размещение в сети *Ethereum* контракта или транзакции с отправителя взимается минимальная фиксированная плата — 21 000 *газ*. Если при реализации байткода контракта выявляется нехватка газа, то виртуальная машина останавливает работу и сообщает об ошибке.

Байткод, выполняемый на *EVM*, не может иметь доступ к внешним ресурсам (файлы и сеть). Такая изолированная среда способствует безопасному выполнению сложных и непроверенных программных кодов.

Важнейшим обстоятельством является то, что виртуальная машина *EVM* реализована на основе стека, ограниченного 1024 элементами. В этом случае любая выполняемая инструкция использует стек, а доступ к размещенным в стеке операндам осуществляется в порядке очереди (режим *LIFO — last in, first out*).

В отличие от виртуальных машин с регистровой организацией, при использовании стека пропадает необходимость в адресации регистров, что значительно упрощает и укорачивает тело команды, снижает сложность вычислительных процедур.

Кроме стека, данные в *EVM* хранятся еще в двух местах.

Первое — это основная память (аналог оперативной памяти в традиционной вычислительной машине). Байткод контракта реализуется только после его размещения в основной памяти, которая очищается, когда байткод контракта завершает выполнение.

Второе место — это постоянное хранилище с адресацией вида «ключ — значение» (аналог дискового накопителя), где размещается код программы контракта. Для пересылки кода программы из постоянного хранилища в основную память используется инструкция *CODECOPY*.

В *EVM* ширина машинного слова составляет 256 *бит* (32 *байт*), что принципиально отличается от обычных значений этого параметра в традиционных процессорах (от 8 до 64 *бит*).

В этом случае при очевидном возрастании алгоритмической сложности выполнения операций происходит существенное сокращение количества обращений к памяти, что значительно снижает время выполнения программы контракта.

Последнее объясняется следующими причинами:

– большая ширина машинного кода для инструкций приводит к сокращению количества используемых команд, упрощает их адресацию, делает команды более «информативными» (в теле команды размещается большее количество управляющих воздействий);
– использование «длинных» операндов приводит к сокращению их количества. Однако если значительная часть обрабатываемых операндов имеет меньшую длину, то это приводит к неэффективному использованию памяти;

– машинный код шириной 256 *бит* более удобен для выполнения криптографических операций (например, вычисления хеш-функции [6]).

Модель информационного взаимодействия постоянного хранилища, основной памяти и стека представлена на рис. 2.

Программный код, содержащийся в постоянном хранилище, пересылается в основную память и подвергается компиляции. Затем происходит последовательное выполнение его инструкций. Инкрементация счетчика программы происходит после чтения из основной памяти очередной инструкции, а обновление содержимого стека — после ее выполнения.

При выполнении очередной инструкции байткода виртуальная машина находится в соответствующем этой инструкции состоянии, которое характеризуется такими параметрами, как объем доступного газа, значение счетчика программы, содержимое стека.

Итератор (см. рис. 2), реализуя свои функции, обеспечивает установление соответствующего состояния *EVM*.

Функциями итератора являются:

– считывание очередной команды байткода из основной памяти;
– выполнение команд PUSH/POP (добавление/удаление элементов стека);
– изменение значения счетчика программы.

Набор команд (операций) виртуальной машины *EVM* составляют команды (операции) разных категорий:

– арифметические, логические, криптографические операции;
– операции, управляющие информацией об окружении, о блоке;
– операции со стеком, памятью, хранилищем, потоком управления;
– операции сохранения, дублирования, замены;
– журнальные операции;
– системные операции.

В *таблице* приведены характеристики арифметических операций: мнемоническое название; значение кода операции; количество элементов, добавляемых в стек (PUSH) и удаляемых из стека (POP); вычислительная сложность выполнения в единицах газа.

В качестве занимательной подробности отметим, что самой сложной является системная операция создания новой учетной записи с заданным кодом. Ее выполнение «стоит» 32 000 единиц газа.

Таблица

Основные характеристики арифметических операций виртуальной машины *EVM*

Название	Значение кода операции	*POP*	*PUSH*	Газ	Описание
STOP	0x00	0	0	0	Останавливает выполнение
ADD	0x01	2	1	3	Сложение двух значений
MUL	0x02	2	1	5	Умножает два значения
SUB	0x03	2	1	3	Операция вычитания
DIV	0x04	2	1	5	Целочисленное деление
SDIV	0x05	2	1	5	Целочисленное деление со знаком
MOD	0x06	2	1	5	Деление с остатком
SMOD	0x07	2	1	5	Деление с остатком и знаком
ADDMOD	0x08	3	1	8	Сложение по модулю
MULMOD	0x09	3	1	8	Умножение по модулю

5. Средства обеспечения информационного взаимодействия смарт-контрактов с внешней средой

Сеть блокчейн, как и любая другая децентрализованная распределенная сеть, действует изолированно от внешнего мира, но при этом во многих случаях должна учитывать изменения условий внешней среды. Самостоятельно получать сведения о таких изменениях сеть не может, поэтому для обеспечения доступа к информационным *off-chain*-ресурсам привлекается третья сторона [14].

Решение проблемы коммутации с реальным миром особенно важно для смарт-контрактов, которые должны контролировать бизнес-логику, учитывать множество факторов и в идеальном случае выполняться автоматически.

Оракулы входят в экосистему смарт-контрактов и используются для предоставления им достоверных и полных сведений об *off-chain*-ресурсах.

Существенно, что оракул является только поставщиком, посредником между источником информации и смарт-контрактом (*рис*. 3.).

В зависимости от реализуемого алгоритма информационного взаимодействия оракулы могут относиться к разным типам:

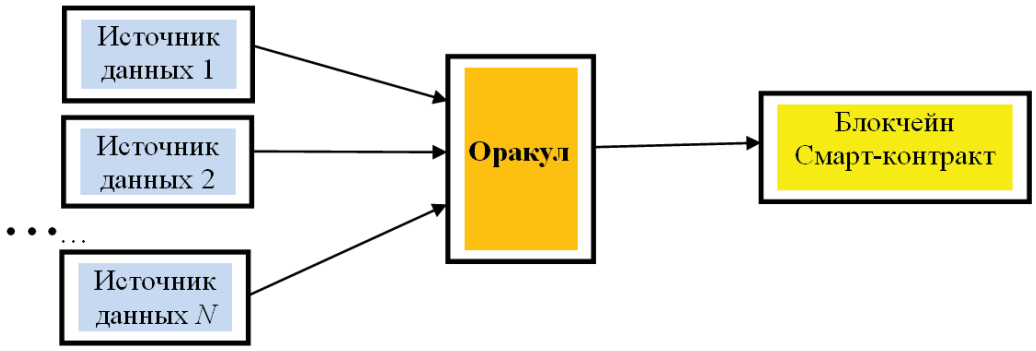

Рис. 3. Модель информационного взаимодействия оракула и смарт-контракта

– программный оракул — существует в виде программного продукта, обрабатывает сетевую информацию, получаемую с сайтов компаний;
– аппаратный оракул — фиксирует совершение событий (сигналов с разнообразных датчиков) и физическое выполнение условий;
– входящий оракул — направляет информацию из внешнего мира внутрь смарт-контракта;
– исходящий оракул — направляет информацию во внешний мир;
– оракул, основанный на консенсусе — предполагает использование не одного, а нескольких оракулов для повышения достоверности и полноты информации.

Услуги оракула могут быть оказаны при обращении к онлайн-сервисам, таким, например, как *www.oraclize.it* и *www.realitykeys.com*.

Сервис *TLSNotary/pagesigner* используется для доказательства подлинности информации, предоставляемой оракулом смарт-контракту. При этом с использованием криптографических методов подтверждается информационное взаимодействие между источником данных и оракулом.

Разработку программных продуктов, реализующих функции блокчейн-оракулов, ведут также такие компании, как *Smart Contract* (проект *ChainLink*), *BNC (BraveNewCoin)*.

Заключение

Таким образом, рассмотрены методы применения программных инструментов, предназначенных для разработки, тестирования, развертывания и применения смарт-контрактов, определены характеристики и особенности использования и алгоритмические возможности языка программирования высокого уровня, предназначенного для разработки смарт-контрактов; выполнен анализ особенностей функционирования и применяемого набора операций виртуальной машины блокчейн-сети; представлена модель информационного взаимодействия постоянного хранилища, основной памяти и стека виртуальной машины блокчейн-сети; исследованы средства обеспечения информационного взаимодействия смарт-контракта с внешней средой.

Литература

1. Блокчейн на пике хайпа. Правовые риски и возможности : монография / А.Ю. Иванов, М.Л. Башкатов, Е.В. Галкова и др. М. : Изд. дом Высшей школы экономики, 2020. 240 с.
2. Бегларян М.Е., Добровольская М.Ю. Блокчейн технология для цифровизации экономики: угрозы и перспективы // Правовая информатика. 2020. № 4. С. 46—54. DOI: 10.21681/1994-1404-2020-4-46-54 .
3. Ващекин А.Н., Дзедзинский А.В. Проблемы правового регулирования отношений в цифровом пространстве // Правосудие. 2020. Т. 2. № 2. С. 126—147. DOI: 10.37399/issn2686-9241.2020.2-126-147 .
4. Королев В.Т., Ловцов Д.А. Качество стандартизованной системы алгоритмов шифрования данных в ГАС РФ «Правосудие» // Правовая информатика. 2018. № 1. С. 49—59. DOI: 10.21681/1994-1404-2018-1-49-59 .
5. Ловцов Д.А. Имплементация «цифровых» прав в экономике: информационно-правовые аспекты // Российское правосудие. 2020. № 10. С. 42—53. DOI: 10.37399/issn2072-909X.2020.10.42-53 .
6. Ловцов Д.А. Теория защищенности информации в эргасистемах : монография. М. : Рос. гос. ун-т правосудия, 2021. 276 с. ISBN 978-5-93916-896-0.
7. Ловцов Д.А. Информационная безопасность автоматизированных блокчейн-систем: угрозы и способы повышения // Тр. II Междунар. науч.-прак. конф. «Трансформация национальной социально-экономической системы России» (22 ноября 2019 г.) / РГУП. М. : РГУП, 2020. С. 464—473. ISBN 978-5-93916-823-6.
8. Ловцов Д.А. Информационно-правовые основы правоприменения в цифровой сфере // Мониторинг правоприменения. 2020. № 2(35). С. 44—52. DOI: 10.21681/2226-0692-2020-2-44-52 .

9. Ловцов Д.А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. 2017. № 3. С. 66—74.
10. Ловцов Д.А., Терентьева Л.В. Правовое регулирование международных коммерческих электронных контрактов. Технологические и правовые аспекты электронной подписи // Lex russica. 2020. Т. 73. № 7. С. 115—126. DOI: 10.17803/1729-5920.2020.164.7.115-126 .
11. Максуров А.А. Блокчейн, криптовалюта, майнинг: понятие и правовое регулирование : монография. М. : Дашков и К. 2020. 198 с.
12. Проблемы создания цифровой экосистемы: правовые и экономические аспекты : монография / Е.Н. Абрамова, А.П. Алексеенко, С.Н. Белова и др. Под общ. ред. В.А. Вайпана, М.А. Егоровой. М. : Юстицинформ, 2021. 276 с.
13. Сажина М.А., Костин С.В. Блокчейн в системе управления знанием : монография. М. : ИНФРА-М, 2021. 90 с.
14. Тебернакулов А., Койфманн Я. Блокчейн на практике. М. : Альпина Паблишер, 2019. 260 с.
15. Управление бизнесом в цифровой экономике: вызовы и решения : монография / Под ред. И.А. Аренкова, Т.А. Лезиной, М.К. Ценжарик, Е.Г. Черновой. СПб. : СПбГУ, 2019. 360 с.
16. Цихилов А.М. Блокчейн: принципы и основы. М. : Интеллектуальная Литература, 2019. 188 с.
17. Черных А.М. Технологии распределенного реестра и защита документооборота судебной системы // Правовая информатика. 2020. № 4. С. 20—28. DOI: 10.21681/1994-1404-2020-4-20-28 .
18. Чурилов А.Ю. Правовое регулирование применения технологии блокчейн : монография. М. : Юстицинформ, 2021. 152 с.

*Рецензент: **Сухов Андрей Владимирович**, доктор технических наук, профессор, старший научный сотрудник научно-производственного объединения «Специальная техника и связь», Российская Федерация, г. Москва.*
E-mail: avs57@mail.ru

INFORMATION AND SOFTWARE ASPECTS OF THE DEVELOPMENT AND APPLICATION OF SMART CONTRACTS

Sergei Fedoseev, *Ph.D. (Technology), Associate Professor, Professor at the Department of Information Technology Law, Informatics and Mathematics of the Russian State University of Justice, Moscow, Russian Federation.*
E-mail: fedsergvit@mail.ru

Keywords: *smart contract bytecode, software tools for developing smart contracts, Ethereum virtual machine, integrated development environments, Solidity programming language, blockchain network oracle, Solidity virtual machine instruction set, stack computer architecture.*

Abstract.
Purpose of the paper: justifying methodological approaches to solving tasks of developing and applying smart contracts.
Methods used: logical modelling of legal and information relations related to using smart contracts, system analysis of the relationships in the subject area of the legal sphere, objects in the information network technologies sphere, software tools, mathematical algorithms, and the main objects and methods of decision theory and set theory.
Results obtained: an analysis of the characteristics and methods of using software tools for development, testing, deployment and application of smart contracts was carried out. The characteristics, features of use and algorithmic capabilities of a high-level programming language designed for the development of smart contracts were determined. An analysis of the features of functioning and applied set of operations of a blockchain network virtual machine was carried out. A model of information interaction of permanent storage, main memory and the stack of a blockchain network virtual machine was presented. Means for ensuring the information interaction of a smart contract with the external environment were studied.

References

1. Blokchein na pike khaipa. Pravovye riski i vozmozhnosti : monografiia. A.Iu. Ivanov, M.L. Bashkatov, E.V. Galkova i dr. M. : Izd. dom Vysshei shkoly ekonomiki, 2020. 240 pp.
2. Beglarian M.E., Dobrovol'skaia M.Iu. Blokchein tekhnologiia dlia tsifrovizatsii ekonomiki: ugrozy i perspektivy. Pravovaia informatika, 2020, No. 4, pp. 46-54. DOI: 10.21681/1994-1404-2020-4-46-54 .
3. Vashchekin A.N., Dzedzinskii A.V. Problemy pravovogo regulirovaniia otnoshenii v tsifrovom prostranstve. Pravosudie, 2020. T. 2, No. 2, pp. 126-147. DOI: 10.37399/issn2686-9241.2020.2-126-147 .

4. Korolev V.T., Lovtsov D.A. Kachestvo standartizovannoi sistemy algoritmov shifrovaniia dannykh v GAS RF "Pravosudie". Pravovaia informatika, 2018, No. 1, pp. 49-59. DOI: 10.21681/1994-1404-2018-1-49-59 .
5. Lovtsov D.A. Implementatsiia "tsifrovykh" prav v ekonomike: informatsionno-pravovye aspekty. Rossiiskoe pravosudie, 2020, No. 10, pp. 42-53. DOI: 10.37399/issn2072-909X.2020.10.42-53 .
6. Lovtsov D.A. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : Ros. gos. un-t pravosudiia, 2021. 276 pp. ISBN 978-5-93916-896-0.
7. Lovtsov D.A. Informatsionnaia bezopasnost' avtomatizirovannykh blokchein-sistem: ugrozy i sposoby povysheniia. Tr. II Mezhdunar. nauch.-prak. konf. "Transformatsiia natsional'noi sotsial'no-ekonomicheskoi sistemy Rossii" (22 noiabria 2019 g.). RGUP. M. : RGUP, 2020, pp. 464-473. ISBN 978-5-93916-823-6.
8. Lovtsov D.A. Informatsionno-pravovye osnovy pravoprimeneniia v tsifrovoi sfere. Monitoring pravoprimeneniia, 2020, No. 2(35), pp. 44-52. DOI: 10.21681/2226-0692-2020-2-44-52 .
9. Lovtsov D.A. Problema garantirovannogo obespecheniia informatsionnoi bezopasnosti krupnomasshtabnykh avtomatizirovannykh sistem. Pravovaia informatika, 2017, No. 3, pp. 66-74.
10. Lovtsov D.A., Terent'eva L.V. Pravovoe regulirovanie mezhdunarodnykh kommercheskikh elektronnykh kontraktov. Tekhnologicheskie i pravovye aspekty elektronnoi podpisi. Lex russica, 2020. T. 73, No. 7, pp. 115-126. DOI: 10.17803/1729-5920.2020.164.7.115-126 .
11. Maksurov A.A. Blokchein, kriptovaliuta, maining: poniatie i pravovoe regulirovanie : monografiia. M. : Dashkov i K, 2020. 198 pp.
12. Problemy sozdaniia tsifrovoi ekosistemy: pravovye i ekonomicheskie aspekty : monografiia. E.N. Abramova, A.P. Alekseenko, S.N. Belova i dr. Pod obshch. red. V.A. Vaipana, M.A. Egorovoi. M. : Iustitsinform, 2021. 276 pp.
13. Sazhina M.A., Kostin S.V. Blokchein v sisteme upravleniia znaniem : monografiia. M. : INFRA-M, 2021. 90 pp.
14. Tebernakulov A., Koifmann Ia. Blokchein na praktike. M. : Al'pina Pablisher, 2019. 260 pp.
15. Upravlenie biznesom v tsifrovoi ekonomike: vyzovy i resheniia : monografiia. Pod red. I.A. Arenkova, T.A. Lezinoi, M.K. Tsenzharik, E.G. Chernovoi. SPb. : SPbGU, 2019. 360 pp.
16. Tsikhilov A.M. Blokchein: printsipy i osnovy. M. : Intellektual'naia Literatura, 2019. 188 pp.
17. Chernykh A.M. Tekhnologii raspredelennogo reestra i zashchita dokumentooborota sudebnoi sistemy. Pravovaia informatika, 2020, No. 4, pp. 20-28. DOI: 10.21681/1994-1404-2020-4-20-28 .
18. Churilov A.Iu. Pravovoe regulirovanie primeneniia tekhnologii blokchein : monografiia. M. : Iustitsinform, 2021. 152 pp.

МЕТОДЫ И ПРОЦЕДУРЫ ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В ЭРГАСИСТЕМАХ

Ловцов Д.А.*

Ключевые слова*: эргасистема, защищенность информации, достоверность, конфиденциальность, сохранность, методы обеспечения, аппаратно-программные процедуры, информационно-распределительная сеть, прагматическая классификация, показатели, критерии, подсистема контроля и защиты информации, организационно-функциональные принципы.*

Аннотация.

Цель работы: совершенствование научно-методической базы теории защищенности информации в эргасистемах.

Методы: системный анализ, формализация сложной задачи, прагматическая классификация и распределение основных методов и аппаратно-программных процедур обеспечения защищенности информации в эргасистемах.

Результаты: определена математическая структура комплексной задачи обеспечения защищенности информации в эргасистемах; определена логическая последовательность методологических этапов разработки подсистемы контроля и защиты информации на основе прагматических организационно-функциональных принципов; обоснована непротиворечивая совокупность методов контроля и защиты информации от ошибок переработки, от разрушающих факторов и от несанкционированного доступа и использования; обоснована прагматическая классификация основных методов и распределение целесообразных сетевых аппаратно-программных процедур обеспечения защищенности информации в эргасистемах.

Полученные результаты являются концептуально-теоретической основой для создания соответствующего эффективного информационно-математического обеспечения контроля и защиты информации в эргасистемах.

DOI: 10.21681/1994-1404-2021-3-34-49

Введение

С учетом обоснованной предметно-логической декомпозиции качества информации [4, 6, 7] решение *комплексной научной проблемы* обеспечения защищенности информации (ОЗИ) в эргасистемах возможно на основе *специальной методологии* контроля и защиты информации (КЗИ), определяющей взаимосвязь трех соответствующих научно-технических проблем: обеспечения *достоверности* (помехоустойчивости, помехозащищенности), *конфиденциальности* (скрытности, доступности, имитостойкости) и *сохранности* (целостности, готовности) информации, отдельных свойств информации и подсистемы КЗИ, основных показателей и критериев оптимизации КЗИ и представляющей собой:

учение (совокупность теоретических положений) о принципах и структурах подсистемы КЗИ, логической организации (технологии) КЗИ, системе способов и методик (методов и показателей) КЗИ, комплексе средств (видов обеспечений) КЗИ;

инструмент (совокупность технических решений), с помощью которого практически решается триединый комплекс научно-технических проблем КЗИ обеспечения достоверности, конфиденциальности и сохранности информации в существующих и перспективных эргасистемах.

Степень обеспечения *защищенности* информации в эргасистеме определяется, таким образом, состоянием решения проблем обеспечения достоверности, конфиденциальности и сохранности информации (контрольно-измерительной, командно-программной, технологической и др. [6]).

Формализация и анализ комплексной задачи обеспечения защищенности информации в эргасистемах

Обеспечение *достоверности* информации заключается в достижении требуемого уровня достоверно-

* ***Ловцов Дмитрий Анатольевич,*** *доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, заместитель по научной работе директора Института точной механики и вычислительной техники им. С.А. Лебедева Российской академии наук, заведующий кафедрой информационного права, информатики и математики Российского государственного университета правосудия, г. Москва, Российская Федерация.*

E-mail: dal-1206@mail.ru

сти путем внедрения методов контроля дестабилизирующих факторов (ДФ) и защиты информации на всех стадиях ее *переработки*[1], повышением надежности комплекса средств автоматизации (КСА) эргасистемы (включая комплексы технических и программных средств — КТС, КПС), административно-организационными мерами (моральным и материальным стимулированием, направленным на снижение числа ошибок, улучшением условий труда персонала, организацией селективного доступа и др.) [6, 7]. Критерии оптимальности при этом, как правило[2] [3] — минимизация:

вероятности (q_1) искажения единичного массива информации (ЕМИ);

суммарного среднего времени $(\Sigma_j t'_j)$ на обработку, контроль и исправление информационного массива (ИМ);

суммарных потерь с учетом затрат $(\Sigma_j c_j)$ на разработку и функционирование структур контроля, исправление ошибок и потери в эргасистеме при использовании недостоверной информации;

времени переработки ИМ и материальных затрат при ограничении на достоверность и др.,

а также — *максимизация* достоверности (D) переработки информации как некоторой функции вероятности (q_1) ошибки.

Обеспечение *конфиденциальности* информации (ОКИ) заключается в обеспечении требуемого уровня конфиденциальности и секретности ИМ путем дополнительного преобразования (семантического, операторного, криптографического, псевдослучайного, организационно-диалогового и др.) *привилегированной* информации, контроля полномочий программно-технических средств, ресурсов эргасистемы и лиц (операторов, персонала, пользователей и др.), взаимодействующих со средствами автоматизации, и разграничения доступа к ИМ. Прагматические критерии оптимальности[3] — *минимизация*:

вероятности (p_o) преодоления («взлома») защиты;

вероятности (p_w) определения пароля значности W по его отображениям;

суммарных $(\Sigma_j c_j)$ затрат (интеллектуальных, финансовых, материальных, временных и др.) на разработку и эксплуатацию подсистемы КЗИ при ограничениях на вероятность $(p_н)$ несанкционированного доступа (НСД);

суммарных $(\Sigma_i r_i + \Sigma_j c_j)$ потерь от «взлома» защиты и затрат на разработку и эксплуатацию соответствующих элементов подсистемы КЗИ и др.,

а также — максимизация ожидаемого безопасного времени $(\check{T}_o)$ до «взлома» подсистемы защиты.

Обеспечение *сохранности* информации (ОСИ) заключается в обеспечении необходимого уровня сохранности ИМ путем введения специальной организации хранения и подготовки, регенерации и восстановления ИМ, использования дополнительных ресурсов для их резервирования, что позволяет значительно уменьшить влияние разрушающих факторов на эффективность функционирования эргасистем в целом. Основные критерии оптимальности[4] [3] — *максимизация*:

вероятности (p_z) успешного решения определенной частной задачи эргасистемы при наличии соответствующих ИМ, их дубликатов, копий и (или) предысторий;

вероятности (p_t) сохранности ИМ за фиксированный интервал t времени их эксплуатации;

вероятности (p_v) восстановления ИМ и др.,

а также — *минимизация*:

среднего времени (t'_z) решения задачи эргасистемы;

среднего времени (t'_v) восстановления ИМ;

стоимостных затрат $(\Sigma_j c_j)$ на дополнительные носители информации для размещения резервных ИМ, потерь от разрушения ИМ и др.

Соответствующую общую математическую постановку задачи обеспечения защищенности информации в эргасистеме с учетом расширенной концепции [4] можно представить[5] в виде композиции математических формулировок частных задач обеспечения достоверности, конфиденциальности и сохранности ИМ соответственно:

$$K\colon F\{\lambda_k, D(S^*), \check{T}_o(S^*), p_z(S^*)\} = \max_{\{S\}}, \qquad (1)$$

$$\Sigma_j t'_j(S^*) \le T^0, \Sigma_i c_{1i}(S^*) \le C_1^{\,0}, j=1,\ldots,J;\ i=1,\ldots,I_1;$$
$$p_w(S^*) \le p_w^{\,0}, \Sigma_i c_{2i}(S^*) \le C_2^{\,0}, w=1,\ldots,W;\ i=1,\ldots,I_2;$$
$$t'_z(S^*) \le t_z^{\,0}, \Sigma_i c_{3i}(S^*) \le C_3^{\,0}, z=1,\ldots,Z;\ i=1,\ldots,I_3,$$

$$S = < S_1, S_2, S_3 >;\ S \in \Delta = \Delta_1 \times \Delta_2 \times \Delta_3$$
$$S_1 = < G, p_i = 1 - q_i, f_j = 1 - e_j, \tau_i, x_i, \vartheta_j, y_j, t_j, z_j, I, J >;$$
$$S_2 = < X, K^0, E, A(R), T, w+r, V >;$$
$$S_3 = < K, \tau, \Pi, N, p, \theta >;$$
$$\lambda_k \ge 0;\ \Sigma_k \lambda_k = 1,$$

где

Δ — множество допустимых решений-троек: структур S_1 переработки информации, наборов S_2 атрибутов доступа к ресурсам эргасистемы, стратегий S_3 сохранения и подготовки ИМ; λ_k, k =1, 2, 3 — весовые коэффициенты;

D — вероятность достоверной переработки ЕМИ в эргасистеме; $\check{T}_o$ — ожидаемое безопасное время работы КСА (время до раскрытия пароля (ключа) доступа); p_z — вероятность успешного решения функциональной задачи эргасистемы;

T^0 — директивное время переработки (обработки, контроля ДФ и исправления ошибок) информации; $C_1^{\,0}$ — заданный материальный ресурс на обработку,

[1] Ловцов Д. А. Защита информации от искажения при переработке // Информатика и образование. 1996. № 3. С. 84—89.

[2] Ловцов Д. А. Контроль и защита информации в АСУ. В 2-х кн. Кн. 1. Вопросы теории и применения. М. : ВА им. Петра Великого, 1991. 172 с.; Кн. 2. Моделирование и разработки. М. : ВА им. Петра Великого, 1997. 252 с.

[3] Там же.

[4] Там же.

[5] Там же.

контроль и исправление ошибочного ЕМИ; t'_z — среднее время функционирования КСА при решении частной задачи эргасистемы; p_w — вероятность НСД (определения пароля (ключа) по его отображениям);

$G = (A, B)$ — ориентированный граф-модель технологического процесса переработки информации (ТППИ) с множеством A, отображающих заданное множество задач переработки информации (ЗПИ), и множеством дуг[6] $B \subseteq A \times A$; p_i, $i = 1,\ldots,I$ — вероятность правильной обработки ЕМИ на i-м этапе ТППИ и, в частности, того, что ИМ-оригинал M_0 не разрушится за единичный интервал времени $t = 1$ при его обновлении; q_i — вероятность искажения ЕМИ; τ_i — время обработки ЕМИ (создания одной копии ИМ M_0); x_i — затраты на обработку ЕМИ; f_j, $j = 1,\ldots,J$ — вероятность обнаружения ДФ (ошибки) в ЕМИ на j-м этапе контроля; e_j — вероятность пропуска ДФ (ошибки); ϑ_j — время контроля ЕМИ; y_j — затраты на контроль ЕМИ; t_j — время исправления ЕМИ на j-м этапе контроля; z_j — затраты на исправление ошибочного ЕМИ; K — количество копий ИМ M_0; Π — количество предысторий ИМ M_0; $N = 1,\ldots,8$ — номер схемы восстановления ИМ;

$X = \{X_i\}$, $i = 1,\ldots,n$ — множество индивидуальных паролей (имен, алгоритмов, вопросов и др.) $X_i = \{x_{ij}\}$, $j = 1,\ldots,w_i$ n объектов эргасистемы; $E = \{E_i\}$, $i = 1,\ldots,n$ — множество соответствующих эталонных паролей, преобразованных [10] с целью защиты по соответствующему ключу $k_i \in K^0$ и хранящихся в специальной памяти эргасистемы; $A(R) = \{A_l(R_l)\}$, $l=1,\ldots,L$ — множество алфавитов различного размера R_l парольных символов $x_{ij} \in A_l(R_l)$; $T = < t_и, t_x, t_о, t_п, t_з >$ — определенное значение длительности цикла доступа, включающей время $t_и$ ввода имени объекта эргасистемы и время t_x ввода пароля, время $t_о$ отключения КСА в случае ошибочного (неверного) ввода, $t_п$ — печати сообщения об ошибке, $t_з$ — искусственной задержки начала следующей попытки; f — заданное значение числа разрешенных попыток доступа; $w+r$ — значность передаваемого сообщения (включая w символов пароля-стринга и r символов (служебных) идентификатора) при попытке получить доступ к ресурсам эргасистемы; V — скорость передачи данных (телеграфирования, если $A_0 = < 0,1 >$) в линии связи, *смв/с* (*бод*);

$\Sigma_i c_{2i} = c_{21} + \check{c}_{22} = c_{21} + g_1(1 - p_w)$ — суммарные затраты и потери эргасистемы на обеспечение конфиденциальности ИМ; c_{21} — затраты, связанные с разработкой и эксплуатацией элементов контроля и разграничения доступа; $\check{c}_{22}$ — математическое ожидание потерь, которые несет эргасистема в результате раскрытия привилегированной информации; g_1 — потери эргасистемы от несанкционированного использования одного ИМ;

$\Sigma_i c_{3i} = c_{31} + \check{c}_{32} = [g_2(t'_z - \theta) + g_3] + g_4(1 - p_z)$ — суммарные затраты и потери эргасистемы на обеспечение сохранности ИМ; c_{31} — затраты, связанные с резервированием ИМ; $\check{c}_{32}$ — математическое ожидание потерь, которые несет эргасистема в результате разрушения ИМ-оригинала M_0 и его копий; g_2 — стоимость единицы машинного времени; $g_3(L)$ — стоимость материального носителя ИМ, зависящая от количества L запоминающих устройств для хранения копий или предысторий ИМ-оригинала M_0; g_4 — потери эргасистемы в результате разрушения ИМ M_0 и его копий; θ — время решения частной задачи эргасистемы.

Совместное решение конкретных частных задач обеспечения *достоверности* (т. е. непосредственного назначения узлов обработки, определения этапов контроля и исправления обнаруженных ошибок, выбора методов обнаружения и исправления ошибок и др.), *конфиденциальности* (т. е. определения атрибутов и длительности цикла доступа, выбора методов контроля и разграничения доступа и др.) ИМ и *сохранности* (т. е. определения схем восстановления и регенерации ИМ, выбора методов резервирования ИМ, обнаружения и исправления ошибок и др.) с использованием рассмотренных в задаче (1) показателей эффективности и качества, а также известного математического аппарата [3, 5, 9, 10, 16, 19] позволит обеспечить требуемый уровень *защищенности* информации в реальной эргасистеме.

Последовательность разработки обобщенной подсистемы КЗИ (рис. 1) в эргасистеме включает ряд этапов оценивания, анализа и обоснования комплекса *средств* и *протоколов* (регламентов и процедур) КЗИ с учетом специфики трех основных научно-технических проблем ОЗИ.

При этом очевидно, что требуемый уровень защищенности ИМ в эргасистеме определяется соответствием между ценностью используемой информации и теми затратами (снижением производительности КСА, дополнительным расходом оперативной памяти КСА и др.), которые необходимы для его достижения. Поэтому разработчику нужен обоснованный показатель экономической эффективности, связывающий требуемый (заданный) уровень защиты и необходимые затраты на ее реализацию.

Можно, например, использовать коэффициент[7] $C_р$ накладных расходов, связанных с функционированием подсистемы КЗИ:

$$C_р = \{\Sigma_k \Sigma_j F(a_k, r_j)\}/\{\Sigma_i \Sigma_j F(m_i, r_j)\}, \quad (2)$$

где $R = \{r_j\}$, $j=1,\ldots,J$ — кортеж ресурсов КСА; $M = \{m_i\}$, $i=1,\ldots,I$ — кортеж системных процедур КСА; $A = \{a_k\}$, $k=1,\ldots,K$ — кортеж системных процедур подсистемы КЗИ $(A \subseteq M)$; F — показатель

[6] Ловцов Д. А. Планирование и прогнозирование процессов обмена привилегированной информацией в сети АСУ // Зарубежная радиоэлектроника. 1996. № 2. С. 7—64; Ситуационное планирование процесса переработки измерительной информации в сети АСУ // Изв. РАН. Теория и системы управления. 1995. № 5. С. 239—247.

[7] Хоффман Л. Дж. Современные методы защиты информации. М. : Сов. радио, 1980. 246 с.

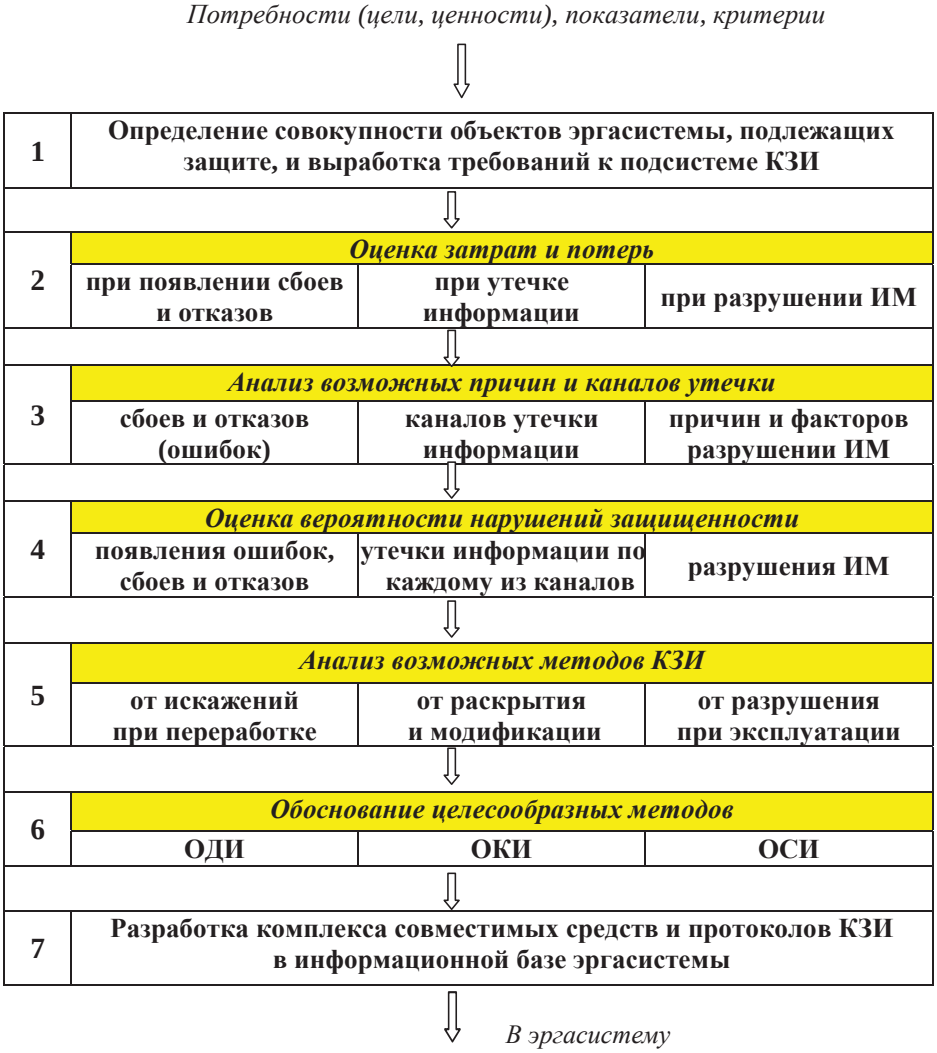

Рис. 1. Логическая последовательность методологических этапов разработки подсистемы контроля и защиты информации

(количественная мера) использования ресурса r_j процедурой m_i или a_k.

При наличии зависимостей типа (2) разработчик может определить процедуры КЗИ и их объемы, которые должны быть использованы в КСА, при этом экономические методы КЗИ дадут накладные расходы, приближающиеся к нулю.

В общем случае применяемая *мера противодействия* (КЗИ) с экономической точки зрения будет приемлема, если эффективность защиты с ее помощью, выраженная через снижение вероятного экономического ущерба, превышает затраты на ее реализацию — так называемый *принцип разумной достаточности*.

Опыт разработки и создания реальных обобщенных подсистем КЗИ в настоящее время еще недостаточен. Вместе с тем известен ряд прагматических *организационно-функциональных принципов*[8] [5, 9] построения подсистем КЗИ, учет которых позволяет уменьшить количество недостатков разрабатываемых подсистем в существующих эргасистемах:

ситуационность (обеспечивает учет сложившейся темпоральной стереотипной ситуации и текущих требований обладателей информации при определении и установлении соответствующего уровня защищенности информации);

целевая эффективность (обеспечивает рациональность использования для защиты информации общесистемных средств и ресурсов);

«тотальность» контроля (обеспечивает всестороннюю проверку возможных традиционных и нетрадиционных каналов доступа к любому защищаемому объекту эргасистемы);

полнота контроля (обеспечивает всестороннюю проверку качества всех ИМ и полномочий любого обращения к любому защищаемому объекту эргасистемы);

простота протоколов КЗИ (обеспечивает отсутствие ошибок проектирования);

обособленность протоколов КЗИ (обеспечивает минимизацию количества объектов эргасистемы, использующих одинаковые параметры и характеристики любого протокола защиты);

[8] Хоффман Л. Дж. Современные методы защиты информации. М. : Сов. радио, 1980. 246 с.;

Шураков В. В. Обеспечение сохранности в системах обработки данных. М. : Финансы и статистика, 1985. 224 с.

несекретность проектирования (обеспечивает выявление и исправление максимального числа «врожденных» недостатков, дефектов и уязвимостей подсистемы КЗИ за счет привлечения различных специалистов);

разделение полномочий (обеспечивает достаточную гибкость и надежность подсистемы КЗИ путем физического разнесения нескольких используемых ключей для открытия процедуры защиты);

минимальность полномочий (обеспечивает использование объектами эргасистемы только тех ИМ, которые необходимы им для выполнения своих функций);

преобладание запретов над разрешениями (обеспечивает доступ и использование ИМ только в случае строгого выполнения определенных условий);

психологическая привлекательность (обеспечивает уменьшение количества попыток лицами, взаимодействующими с комплексом (ЛВК) средств автоматизации, искать обходные пути для доступа к ИМ и их использования).

Методы обеспечения достоверности информации

Использование методов обеспечения достоверности информации (ОДИ) требует введения в структуры переработки ИМ информационной, временной или структурной избыточности.

Структурная избыточность характеризуется введением в состав эргасистем дополнительных элементов (резервирование ИМ, реализация одной функции различными процедурами, схемный контроль в КТС и др.). *Временная* избыточность связана с возможностью неоднократного повторения определенного контролируемого этапа (фазы) переработки информации. *Информационная* избыточность характеризуется введением дополнительных информационных разрядов в используемые ИМ и дополнительных операций в процедуры переработки ИМ, имеющих математическую или логическую связь с алгоритмом переработки, обеспечивающих в результате применения выявление и исправление ошибок определенного типа. Наряду с такой информационной избыточностью, называемой *специальной*, используется и *естественная*, характеризуемая наличием ИМ, логическая связь между которыми позволяет судить об их достоверности.

Известные[9] методы обеспечения (повышения) достоверности перерабатываемой информации в эргасистеме можно разделить (по виду реализации) на две основные группы (рис. 2): организационные (системные и административные); технические (программные и аппаратные).

Организационные методы повышения достоверности состоят в создании и использовании рациональной технологии процесса переработки информации, предусматривающей профилактические меры по снижению доли ошибок переработки до определенного допустимого уровня.

Методы обеспечения надежности (см. *рис.* 2) КСА включают две большие группы методов обеспечения надежности КТС и КПС.

Надежность КСА — свойство КСА выполнять заданные функции, сохраняя во времени значения установленных эксплуатационных показателей в заданных пределах, соответствующих заданным режимам и условиям использования, технического обслуживания, ремонта, хранения и транспортирования. Надежность КТС определяется в основном *случайными* сбоями и отказами, а *надежность* КПС — наличием, как правило, систематических ошибок, допущенных при его разработке. При этом отказ (сбой) технического средства зависит от времени [4] и не зависит от перерабатываемой информации, а программные ошибки являются функцией от текущей входной информации и текущего состояния эргасистемы.

В связи с этим для ОДИ в эргасистеме используются общие типовые методы [14] обеспечения надежности аппаратуры, целью которых является поддержание характеристик КТС эргасистемы в заданных пределах.

Достижения в области повышения надежности КПС в настоящее время гораздо менее ощутимы, чем в надежности КТС, ввиду большой физической сложности КПС, зависимости его от предметной области применения, примитивности «комплектующих» стандартных блоков (операторов языка, сегментов старых программ и др.) с точки зрения конечного результата (единого целого).

Основными методами повышения надежности КПС являются методы контроля его качества, включающего три перекрывающиеся стадии: *отладку, тестирование* (с локализацией и исправлением ошибок) и формальное *доказательство* корректности КПС (соответствия программных компонентов формальным требованиям и логическим утверждениям технического проекта или задания).

Тестирование КПС включает проведение следующих работ[10]:

проектирование набора тестовых комбинаций на основе анализа внешних спецификаций и компонентов КПС, предусматривающее разработку проверочных тестов для логической схемы компонентов (модулей) КПС на чувствительность к различным входным характеристикам; каждого условия и варианта данных; границ всех заданных интервалов на входе и выходе; границ обрабатываемых ИМ для неверных условий и др.;

написание и проверка программ-тестов, предназначенных для тестирования единичных модулей, функционального тестирования (не в рабочих условиях), системного тестирования (в экстремальных режимах функционирования в рабочих или эксплуата-

[9] Мельников Ю. Н. Достоверность информации в сложных системах. М. : Сов. радио, 1974. 192 с.

[10] Шураков В. В. Обеспечение сохранности в системах обработки данных. М. : Финансы и статистика, 1985. 224 с.

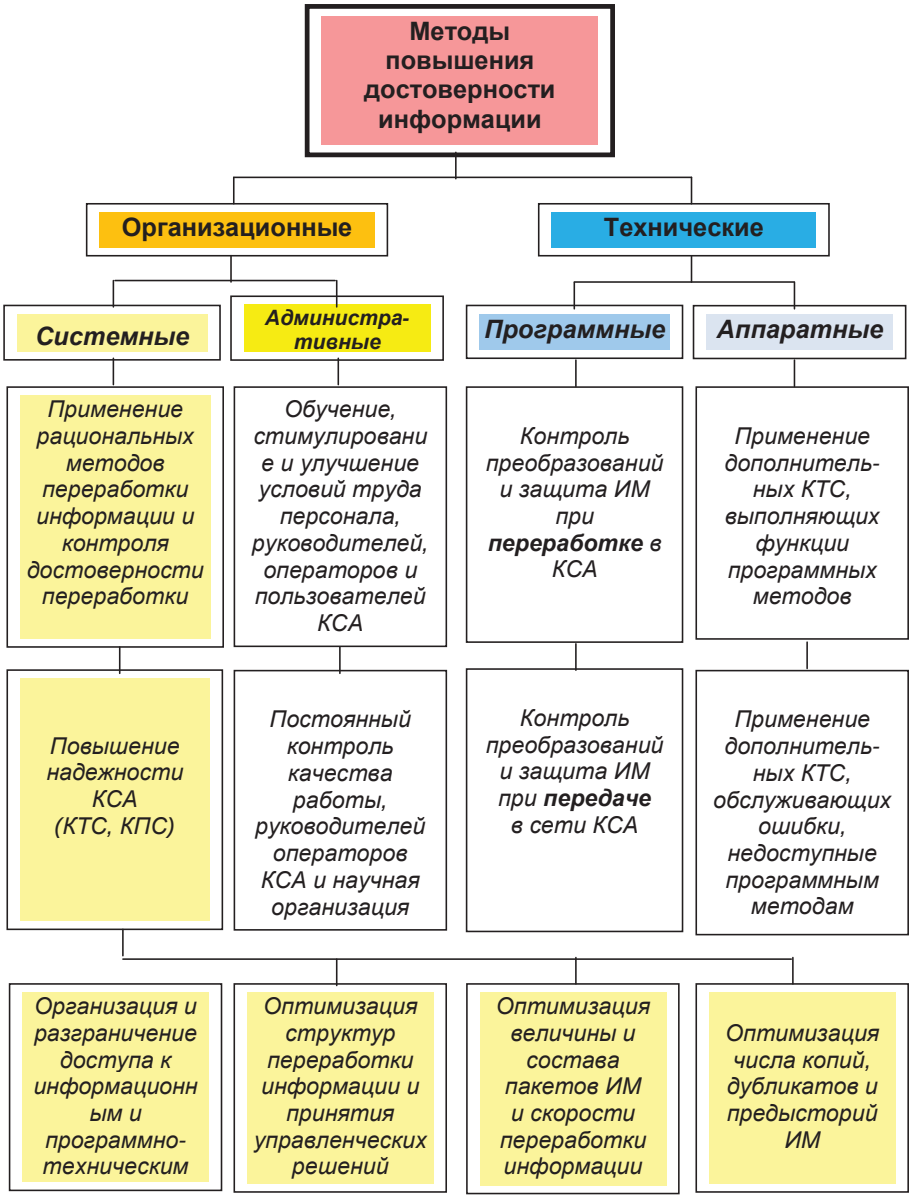

Рис. 2. Общая классификация методов повышения достоверности информации в эргасистемах

ционных условиях), приемо-сдаточного тестирования (в эксплуатационных условиях);

выполнение тестирования (модулей КПС, функционального, системного, приемо-сдаточного и установочного).

Технические методы повышения достоверности перерабатываемой в эргасистеме информации представляют собой совокупность программных и аппаратных методов контроля и выявления ошибок в исходных и получаемых ИМ, их локализации и исправления.

Программные методы включают методы контроля преобразований и защиты ИМ при переработке и методы КЗИ, передаваемой в подсистеме информационного обмена эргасистемы. Программные методы предусматривают дополнительные операции в процедурах переработки информации, которые имеют математическую или логическую связь с алгоритмом переработки информации (преобразования и передачи ИМ). Сравнение результатов этих дополнительных операций с результатами переработки информации дает возможность установить с определенной вероятностью наличие или отсутствие ошибок, а также исправить обнаруженную ошибку.

Аппаратные методы повышения достоверности выполняют практически те же функции, что и программные методы, кроме того, позволяют обнаруживать ошибки ближе к месту их возникновения, а также ошибки, недоступные для программных методов (например, перемежающиеся ошибки). Ими можно пользоваться для представления ЛВК более точной информации об искажениях, вызванных неисправностью КТС.

Сравнение программных и аппаратных методов повышения достоверности показывает, что при относительно сжатых сроках разработки эргасистемы максимальная (заданная) достоверность перерабатываемой информации достигается при использовании

комплекса организационных и программных методов повышения достоверности. Однако параллельно следует работать и над развитием аппаратных методов, новых КТС переработки ИМ, а также моделей и алгоритмов переработки информации и контроля ее достоверности. Анализ методов и определение оптимальной их комбинации, максимизирующей достоверность переработки информации, целесообразно проводить на основе аппарата математического программирования[11] с учетом ограничений на материальные и временные затраты при обеспечении заданного уровня достоверности.

Кроме того, выбор комбинации методов ОДИ определяется технологией переработки информации в эргасистеме, используемыми моделями возникновения ошибок и их взаимодействия, в результате анализа которых рассчитываются вероятности обнаружения и исправления ошибок для различных вариантов структур переработки информации и методов обеспечения требуемого уровня достоверности.

Методы обеспечения конфиденциальности информации

Множество методов ОКИ в эргасистеме можно разделить (по виду реализации) на две основные группы[12] [13, 18] (рис. 3):

организационные (80%), включая административные (50%), физические (22%), законодательные (8%);

технические (20%), включая аппаратные, программные, криптографические.

Административными методами в эргасистеме называется комплекс организационно-правовых мероприятий, регламентирующих (на основе нормативных правовых актов) процессы функционирования эргасистемы, использование ее КТС и информационно-программных ресурсов, а также взаимоотношения ЛВК и эргасистем с целью исключения возможности или существенного затруднения НСД к ИМ. Административные методы ОКИ играют большую роль в создании надежной подсистемы КЗИ от НСД и несанкционированного использования (НСИ), обеспечивая объединение всех организационно-технических средств в единое целое, поскольку возможности НСИ в значительной мере обусловливаются нетехническими аспектами: злоумышленными действиями, нерадивостью или небрежностью ЛВК и др. При помощи административных методов создается необходимая совокупность организационных, организационно-технических, организационно-правовых и др. мероприятий, охватывающая все структурные элементы эргасистемы на всех этапах ее жизненного цикла и приводящая к минимуму (исключающая) возможность утечки информации. Основными *мероприятиями* в такой совокупности являются следующие:

мероприятия при проектировании, строительстве и оборудовании объектов (центров, периферийных элементов и др.) эргасистем по исключению влияния стихийных бедствий, возможностей тайного проникновения в помещения, по обеспечению удобств для контроля прохода и перемещения людей и др.);

организация противопожарной службы;

подбор и подготовка персонала эргасистем (проверка принимаемых на работу, создание условий и стимулирование персонала, обучение правилам работы с привилегированной (закрытой и др.) информацией, ознакомление с мерами ответственности за нарушение правил защиты и др.);

организация надежного пропускного режима;

организация хранения, выдачи и использования документов и носителей информации (определение соответствующих правил, маркировка, ведение журналов выдачи и использования и др.);

организация работы в дежурных сменах эргасистем (выделение ответственных за ОЗИ или создание специальной штатной службы, организация контроля за работой персонала, ведение журналов работы, уничтожение в установленном порядке производственных отходов и др.);

контроль внесения изменений в математическое и программное обеспечение (строгое санкционирование, рассмотрение и утверждение проектов изменений, проверка всех изменений на удовлетворение требованиям ОКИ, документальное отображение изменений и др.);

организация подготовки и контроля работы ЛВК;

планирование мероприятий по ОКИ.

Физическими методами ОКИ в эргасистеме называется комплекс мер и мероприятий, предназначенных для создания физических препятствий (на основе применения различных специальных устройств и сооружений) для потенциальных нарушителей на пути в места, в которых можно иметь доступ к защищаемой информации. Они играют важную роль в комплексе мероприятий по ОКИ, затрудняя использование и прямых, и косвенных каналов утечки информации путем:

физической изоляции сооружений, в которых размещены КСА, от других сооружений;

ограждения территории объектов (элементов и каналов связи) эргасистем заборами (стенами) на расстояниях, достаточных для исключения эффективной регистрации электромагнитных излучений (ЭМИ);

контроля территорий объектов эргасистем;

создания контрольно-пропускных пунктов у входов в помещения объектов эргасистем для проверки ЛВК с точки зрения идентичности, аутентичности и наличия полномочий;

оборудования входных дверей специальными (кодовыми) замками, позволяющими регулировать доступ в помещения;

---

[11] Ловцов Д. А., Князев А. Г. Оптимизация структуры достоверной переработки информации // НТИ. Сер. 3. Информ. процессы и системы. 1998. № 10. С. 20—27.

[12] Там же. Хоффман Л. Дж. Современные методы защиты информации. М. : Сов. радио, 1980. 246 с.

оборудование окон специальными средствами и материалами, не позволяющими осуществлять наблюдение за работой персонала и функционированием КТС;

оборудование дверей и створок шкафов аппаратуры специальными устройствами (механическими, электромеханическими, электронно-механическими и др.), препятствующими НСД;

организации системы охранной сигнализации.

Физические меры ОКИ должны быть предусмотрены для зон, откуда отправляют исходящие и где получают входящие документы, комнат программистов, полок в местах расположения вынесенных терминалов, погрузочных тележек, емкостей для транспортировки ИМ и др., т. е. там, где возможен ввод или вывод привилегированной информации.

Законодательные методы — это комплекс мер, определяемых законами страны, указами руководящих органов и соответствующими положениями, регламентирующими правила переработки и использования информации ограниченного доступа и распространения, а также ответственность за их нарушения, препятствуя тем самым НСИ [15].

Кроме того, для создания соответствующей законодательной защиты конфиденциальности информации в эргасистеме можно применять обычные положения об охране авторских прав, положение о выдаче лицензий, разрешений на снятие копий или сдачу в аренду и наложение требования о вручении в нераспечатанном виде. В качестве *дополнительных* технических мер можно использовать либо нанесение на носитель только объектного кода, либо переключение индивидуальных ИМ для прогона только на определенных центральных процессорах КСА (если их могут однозначно идентифицировать ИМ), либо включение нефункциональных (пустых) подпрограмм в ИМ ЛВК, обеспечивающих внесение искажений в случае неавторизованного использования и др.

Дополнительно к административным правилам часто используются *этические кодексы* поведения [8], определяющие профессиональные идеалы (этические соображения) и позволяющие повысить бдительность, внимательность и организованность персонала эргасистем и их информационно-распределительных сетей (ИРС).

Аппаратными (схемными) методами ОКИ называется комплекс технических мероприятий по разработке и использованию специальных схем и устройств КЗИ (электронных, электронно-механических, электронно-оптических и др.), встроенных конструктивно в серийные образцы технических средств эргасистем или самостоятельных (в составе КТС), позволяющих изолировать ЛВК друг от друга и от операционной системы КСА, обеспечивая при этом возможность эффективного контроля операций по переработке ИМ и уменьшая тем самым вероятность НСИ.

Основными методами аппаратного ОКИ в эргасистемах являются мероприятия по защите информационных массивов в КСА, т. е. в информационно-вычислительных комплексах (ИВК), комплексах командно-измерительных средств (ККИС), комплексах сбора и подготовки информации (КСПИ), комплексах отображения информации (КОИ), а также в каналах связи (КС) и передачи данных, в базах данных и знаний (БДЗ).

Аппаратные методы ОКИ широко применяются в современных эргасистемах, главным образом благодаря их надежности, однако исключительное использование данных методов нецелесообразно по экономическим соображениям (из-за высокой стоимости аппаратных средств и низкой их *адаптируемости* к изменяющимся условиям эксплуатации эргасистем). Состав, типы (общие, специфические или др.) и виды аппаратных методов и средств ОКИ определяются организационно-технической, функциональной и информационной структурами конкретных эргасистем. К настоящему времени разработано значительное число аппаратных средств различного назначения, при этом наибольшее распространение получают следующие[13] [16]:

специальные регистры для хранения реквизитов КЗИ (паролей, идентифицирующих кодов, грифов или уровней секретности и др.);

генераторы кодов для автоматического генерирования идентифицирующего кода устройства (терминала и др.) при включении его в работу и обращении к ресурсам эргасистемы или ИМ коллективного пользования;

устройства считывания кодов с перфокарт или магнитных карт, агрегируемые с замками включения технических средств в работу;

устройства измерения индивидуальных характеристик человека (голоса, узора папиллярных линий, длины пальцев и др.) с целью его идентификации [10];

схемы контроля границ адреса запоминающего устройства с целью определения законности обращения к заданному полю памяти;

схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных [14];

специальные биты секретности, значение которых определяет уровень секретности ИМ, хранимых в той части запоминающего устройства, которой принадлежат данные биты.

Вспомогательные аппаратные средства обеспечивают уничтожение использованных ИМ на магнитных носителях, сигнализируют о попытках несанкционированных действий и др. Особую группу аппаратных средств, получившую наибольшее распространение, составляют устройства преобразования информации.

Программными методами ОКИ (*рис*. 3) называется комплекс специальных алгоритмов и компонентов общего программного обеспечения эргасистем, предназначенных для выполнения функций контроля, разграничения доступа и исключения НСИ.

Программные методы являются наиболее распространенными методами ОКИ вследствие их универ-

[13] Там же.

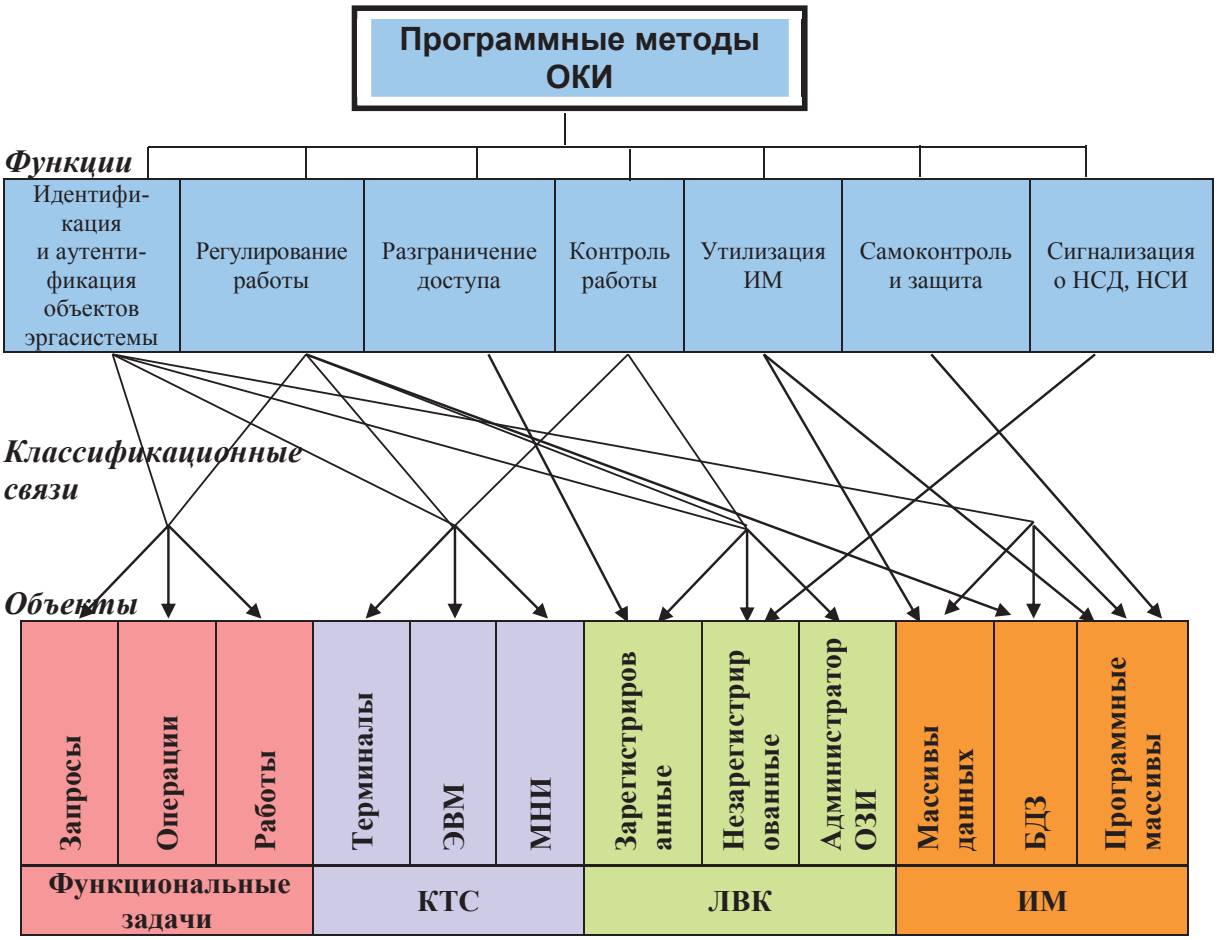

Рис. 3. Общая классификация программных методов обеспечения конфиденциальности информации в эргасистемах

сальности, гибкости, простоты реализации, возможности развития и адаптации к изменяющимся условиям эксплуатации эргасистем и др. Однако они имеют ряд *недостатков*, таких как расходование ресурса ЦП КСА на их функционирование, возможность несанкционированного изменения, невозможность их реализации там, где отсутствует процессор, и др. Программная защита, как правило, применяется там, где введение и использование других методов и средств КЗИ затруднено. По функциональному назначению множество существующих программных методов можно разделить на несколько групп (см. *рис.* 3).

Контроль и защита программных массивов осуществляется путем проверок по контрольным суммам, перезагрузки, организации точек входа, дублирования, криптографического закрытия, модульного диалога и др.

Вспомогательные программы КЗИ обеспечивают уничтожение остаточной информации на магнитных носителях, категорирование «грифованной» информации, формирование грифа секретности выдаваемых документов, имитацию работы с нарушителем для отвлечения его внимания и накопления сведений о характере запросов, ведение регистрационных журналов (для каждого запроса фиксируется выделяемое КСА время, ИМ, используемый терминал, суть запроса или задания, а также информация о том, был разрешен доступ или нет), общий контроль функционирования подсистемы ОКИ, программные проверки для КЗИ при схемных и программных сбоях и др. Особую группу, как и в случае с аппаратными методами, составляют программы преобразования (шифрования и кодирования) информации.

Криптографические методы ОКИ в эргасистемах — это комплекс процедур и алгоритмов преобразования информации, обеспечивающих скрытие смыслового содержания ИМ [1, 19] (*рис.* 4).

Криптографическое закрытие на основе шифрования и кодирования ИМ в эргасистемах исследуется в настоящее время по следующим основным *направлениям* [9, 11, 12]: выбор *рациональных* (надежных) систем и методов шифрования; обеспечение оптимального сочетания требований по *производительности* (быстроте передачи информации) и *криптостойкости* криптографических алгоритмов путем перехода к быстрым алгоритмам электронной подписи, основанным на принципиально других методах расчета (например, на теории графов вместо модульной арифметики); обоснование путей реализации систем шифрования в эргасистемах; разработка правил использования криптографических методов в процессе функционирования эргасистем; оценка эффективности криптографической защиты.

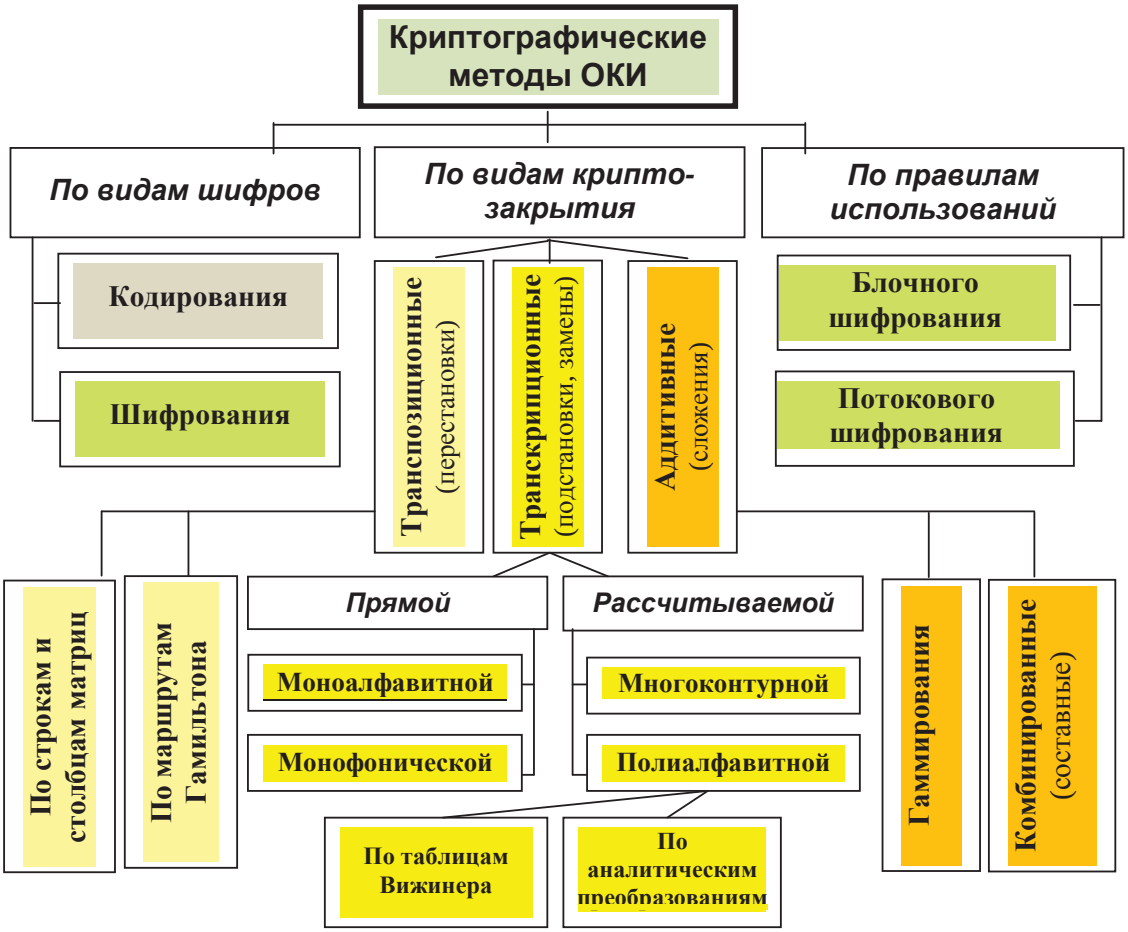

Рис. 4. Общая классификация криптографических методов обеспечения конфиденциальности информации в эргасистемах

Методы обеспечения сохранности информации

Методы обеспечения сохранности ИМ в эргасистеме относятся в основном к области организации и эксплуатации *внутримашинной информационной базы* [6] эргасистемы, реализованной на магнитных носителях, как правило, в виде комплекса функциональных баз данных и знаний (БДЗ).

Организация хранения и использования *статической* информации в БДЗ эргасистемы имеет свои специфические особенности [6], в частности, множество ИМ включает общие, групповые и индивидуальные (личные), что обусловливает необходимость создания гибкой защиты информации, учитывающей особенности использования различных ИМ. Для обеспечения гибкой защиты ИМ необходимо, чтобы система управления БДЗ (СУБД) допускала как частично совпадающие, так и даже противоположные друг другу требования по защите ИМ для различных ЛВК. При отсутствии единых представлений о структуре БДЗ отдельные ЛВК, не зная спецификаций защиты, установленных администратором, могут не получить доступа к данным. В СУБД, кроме стандартных атрибутов ИМ, учитываются и семантические отношения между ними. Эффективность защиты ИМ существенно зависит от способности СУБД обрабатывать отношения. Последние чувствительны к контексту, в котором связанные ИМ появляются, поэтому для организации защиты ИМ необходимо, чтобы СУБД умела их распознавать.

Известные[14] [3] методы повышения сохранности накапливаемой в БДЗ информации можно разделить (*по виду реализации*) на организационные (системные и административные) и технические (программные и аппаратные).

Организационные методы повышения сохранности (рис. 5) состоят в создании и использовании рациональной технологии эксплуатации (хранения и применения) ИМ, предусматривающей профилактические меры по снижению доли искажений ИМ до определенного допустимого уровня и обеспечению своевременного предоставления необходимых аутентичных ИМ для автоматизированного решения задач эргасистемы.

Административные методы научной организации труда (НОТ) персонала эргасистем предусматривают реализацию ряда *принципов*, обеспечивающих уменьшение возможностей нарушения (со стороны персонала) требований сохранности ИМ, основные из которых:

[14] Мамиконов А. Г., Кульба В. В., Шелков А. Б. Достоверность, защита и резервирование информации в АСУ. М. : Энергоиздат, 1986. 304 с.

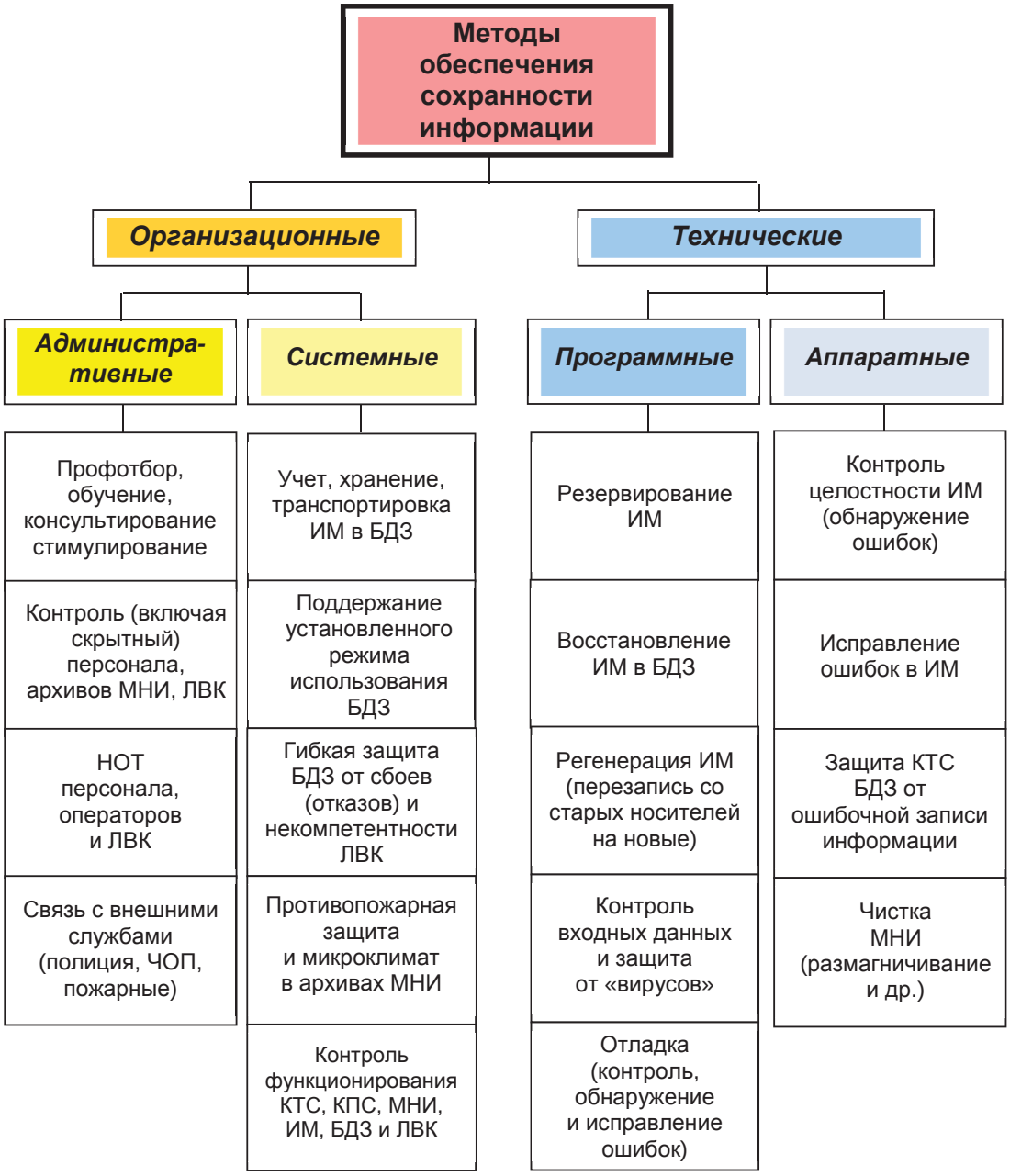

Рис. 5. Общая классификация методов обеспечения (повышения) сохранности информации в эргасистемах

минимизация сведений и данных, доступных персоналу;

минимизация связей (контактов) персонала;

дублирование контроля важных операций (обеспечивает, кроме того, повышение надежности выполнения ответственных операций, и, как следствие, уровня сохранности информации).

Существует также большое количество *аппаратных* (схемных) методов обнаружения ошибок и искажений ИМ (см. *рис.* 5) путем контроля магнитных носителей информации (МНИ), причем при рациональной комбинации подобных методов можно решить задачу защиты ИМ от разрушения при эксплуатации. Данные методы реализуются, как правило, в аппаратном варианте, но часто и в виде программных модулей.

Получение контрольных сумм. В качестве дополнительной избыточной информации для проверки *целостности* ИМ может использоваться сумма всех символов (хранимая в конце ИМ), полученная циклическим сложением после обновления на законном основании. Может также использоваться обратная величина контрольной суммы, при этом сумма всей информации блока ИМ и обратной величины всегда равна нулю.

Для обнаружения искажающих ИМ M_0 простых перестановок (транспозиции) символов (контрольная сумма остается прежней) на практике используются более сложные алгоритмы подсчета контрольной суммы (например, с учетом номера позиции символа). Кроме того, с целью скрытия значения контрольной

суммы она может подвергаться различным защитным преобразованиям.

Использование контрольных чисел. В качестве дополнительной избыточной информации для проверки целостности ИМ может использоваться цифра (хранимая в конце ИМ), связанная с символами ИМ некоторым соотношением. Например, контрольной цифрой может быть остаток от деления контрольного числа на 11, если используется схема сравнения по mod 12.

Использование избыточных кодов — обычно в конце ИМ большого размера вводятся дополнительные контрольные биты (8 или 16), которые позволят выявить, а иногда и автоматически исправить имеющиеся в ИМ ошибки. Схемы, реализующие данный метод, наиболее сложны.

Для магнитных дисков и барабанов *защита записи* обычно проводится на уровне дорожек и на уровне физической записи. Разрешение или запрещение записи на всех дорожках осуществляется *специальными переключателями* на панели управления накопителями. Для частичной защиты жесткого МНИ (диска) обычно его разбивают (с помощью специальных программ) на несколько частей — «самостоятельных» (логических) дисков со своими именами. При этом некоторые из них временно делают доступными только для чтения, чтобы защитить ИМ от изменения, в частности, от «заражения» или порчи «компьютерным вирусом»[15] [17].

Для магнитных флеш-накопителей и карт памяти с этой целью используется переключатель для блокировки устройства от записи, обеспечивающий защиту от несанкционированных корректировок, ошибочных действий, «вирусов» и др. и сохранность программ и данных, которые используются без изменений. Для гибких магнитных дисков — используется специальная *прорезь защиты* (если эту прорезь заклеить, то на дискету нельзя будет произвести запись).

Для магнитных лент используется специальное кольцо защиты от случайной или некомпетентной записи, при отсутствии которого запись на ленту невозможна, поскольку кнопка, отключающая при нажатии схему защиты записи, входит в освободившееся от кольца концентрическое пространство катушки.

Программная проверка по четности, использующая специальную команду «чтение с контролем», реализует контроль только что записанных ИМ без их пересылки в оперативное запоминающее устройство и обеспечивает более качественный контроль по сравнению со *схемной проверкой четности* для каждого бита (слова) при считывании (так как последняя не выявляет ошибок в случае четного количества неверных битов). Частные случаи метода: проверка горизонтальной четности с помощью одного контрольного символа (слова) в конце записи (блока записей); проверка диагональной четности — биты четности соответствуют четности, подсчитываемой по всем диагональным линиям.

Использование счетчиков и порядковых номеров при вводе-выводе и подготовке ИМ. При выполнении операций ввода-вывода обычно подсчитываются ЕМИ (информационные блоки, записываемые на магнитный носитель, считываемые перфокарты и др.). Итоговое значение счетчика документируется и добавляется в ИМ (файл) с целью контроля. При подготовке ИМ на перфокартах с целью контроля полноты файла или выявления нарушений в порядке следования перфокарты нумеруются.

Контроль верности входных ИМ используется в программах ЛВК.

Алгоритмы, реализующие данный метод, достаточно просты. Например, проверку значений цифровых данных осуществляют на основе контроля допустимого диапазона изменения некоторого количественного показателя (например, вероятность не может быть равна 1,5; скорость движения управляемых объектов не может превышать 3×10^6 *м/с* и др.) или показателя логичности (количество решаемых функциональной подсистемой эргасистемы задач не может быть меньше количества ее функций).

Методы восстановления информации в буферном запоминающем устройстве эргасистемы предусматривают использование резервных ИМ, хранящихся на носителях различного типа и вида (магнитных дисках, магнитных барабанах, магнитных лентах, перфокартах и пр.) [3]. Традиционным для МНИ является ***метод восстановления с циклическим оперативным копированием*** ИМ (через определенные промежутки времени) на контрольные носители по схеме «дед — отец — сын». ИМ «сын» (M_0) является последней текущей версией, ИМ «отец» (предыстория Π_{-1} ИМ M_0) отличается от предыдущего на одну выполненную работу с ИМ, а ИМ «дед» (предыстория Π_{-2} ИМ M_0) — на две.

Выбор метода восстановления ИМ определяется структурой эргасистемы, типом контроля, организацией файлов, частотой обновления, соотношением объемов используемых и неиспользуемых данных, ценностью информации, максимально допустимым временем восстановления и др.

При повышенных требованиях к *сохранности* информации может возникнуть необходимость в использовании более одной резервной копии ИМ, которые должны храниться в специальном безопасном месте.

Для повышения уровня *целостности* ИМ в БДЗ используется также большой набор вспомогательных программ обслуживания БДЗ (некоторые из них могут не включаться в СУБД)[16]:

ведения системного журнала КСА (фиксирования сведений об изменениях ИМ для упрощения контроля сохранности БДЗ);

разгрузки (копирования БДЗ для последующего ее восстановления);

восстановления (возврата содержимого БДЗ и системного журнала в начальные до внесения изменений

[15] Ловцов Д. А. Защита информации от компьютерных вирусов // Информатика и образование. 1996. № 4. С. 121—128.

[16] Шураков В. В. Обеспечение сохранности в системах обработки данных. М. : Финансы и статистика, 1985. 224 с.

состояния после сбоев КСА по копиям, полученным в результате работы программы разгрузки);

отката (возврата в исходное положение БДЗ в результате фиксирования незаконных или ошибочных операций над ИМ);

контрольных точек и повторного исполнения (отката только до последней контрольной точки вместо возвращения на общее начало с целью уменьшения непроизводительных затрат времени);

выявления нарушений ограничений *целостности* БДЗ после каждого внесения изменений в ИМ с вызовом программ отката для выхода на исходный рубеж и печатью сообщения об ошибке.

Распределение методов и процедур обеспечения защищенности информации в сети эргасистемы

К штатным аппаратно-программным процедурам (номера приведены в *таблице*) ОЗИ информационно-распределительной сети эргасистемы относятся следующие[17] [2].

1. Криптографическое преобразование (для обеспечения скрытности информационного массива-сообщения (ИМ) или информации о трафике, а также для дополнения ряда других процедур защиты). Возможны симметричное (с использованием тайных ключей) и асимметричное (с использованием известного и индивидуального ключей) преобразования ИМ. При этом степень защиты при помощи криптографического преобразования в значительной мере определяется способом распределения ключей.

2. Управление доступом (для предотвращения несанкционированных попыток доступа к ресурсам подсети, выдачи предупреждения ЛВК (субъекту доступа), и регистрации события в системном журнале для последующего анализа). Используется идентификация логического объекта или информация о нем (пароль и др.) для проверки его полномочий.

3. Обеспечение целостности информационных массивов (массивов данных и программных массивов). Целостность ИМ обеспечивается добавлением к нему при передаче величины, которая является функцией самих данных. На принимающей стороне генерируется такая же величина и сравнивается с принятой. Обнаружение на соответствующем уровне архитектуры взаимодействия абонентов сети несовпадения двух величин может вызвать выполнение процедуры восстановления на этом же или более высоком уровне.

4. Обмен «идентификацией» (для установления или отклонения (завершения) соединения пары информационных узлов (эргасистем) с выдачей сообщения о соответствующем событии). Используются пароли, криптоалгоритмы в сочетании с протоколами «рукопожатия» или взаимной идентификации и аутентификации (для защиты от переадресации), а также характеристики и взаимоотношения подчиненности логических объектов.

5. Заполнение трафика или маскирующий обмен (для защиты от попыток анализа трафика). Процедура эффективна только в случае преобразования всего трафика, когда нельзя отличить информацию от заполнения.

6. Управление маршрутизацией (для использования только безопасных с точки зрения защиты информации подсетей, участков приема, звеньев). Возможно запрещение передачи некоторых ИМ по определенным маршрутам. Оконечный абонент, обнаружив манипуляцию с его ИМ, может потребовать изменить маршрут доставки данных.

7. Цифровая сигнатура. Процесс формирования сигнатуры ИМ при передаче основан на вычислении его криптографической контрольной суммы с использованием индивидуального ключа субъекта (или на преобразовании ИМ). При проверке сигнатуры в принятом ИМ используются типовые (общепринятые) процедуры и информация, из которых нельзя получить привилегированную информацию первого процесса. Существенной характеристикой этого процесса является то, что сигнатура может быть проверена впоследствии третьей стороной.

8. «Нотариальное» заверение (для подтверждения целостности ИМ, удостоверения абонента-источника и абонента-получателя ИМ, регистрации времени сеанса связи и др.), обеспечивается третьей стороной — «нотариусом».

9. Фильтрация информации по принятым в эргасистеме правилам. Основными средствами являются сетевые защищенные экраны (брандмауэры), применяемые на канальном (экранирующий *концентратор*), сетевом (экранирующий *маршрутизатор*), транспортном (транспортный экран) и прикладном (прикладной *экран*) уровнях, обеспечивая предотвращение НСД к ресурсам подсети извне.

Как видно из *таблицы*, на двух нижних уровнях применяется только «позвенное» или канальное (*link-by-link*) преобразование потока данных (т. е. проходящих через звено — *data link*), реализуемое с помощью протокола канального уровня. Способ «позвенного» преобразования имеет следующие особенности:

защищается вся передаваемая по каналу связи информация, включая служебную;

вскрытие ключа шифрования для одного канала не приводит к компрометации информации в других каналах;

все передаваемые ИМ оказываются открытыми на промежуточных узлах — ретрансляторах, шлюзах и др.;

субъект не принимает участия в выполняемых операциях;

для каждой пары узлов требуется свой ключ;

алгоритм шифрования должен обладать достаточно высокой стойкостью и обеспечивать скорость шифрования на уровне пропускной способности канала,

[17] Методические материалы и документация по пакетам прикладных программ. Вып. 57. Телеобработка данных и вычислительные сети / Под ред. В. П. Данилочкина, В. К. Щербо. М. : МЦНТИ, 1988. 342 с.; Ловцов Д. А. Распределение методов и процедур обеспечения за¬щищённости информации в АСУ // Вопросы защиты информации. 1996. № 4. С. 20—24.

Таблица

Распределение методов и процедур КЗИ по стандартизованным уровням *ISO/OSI* архитектуры сети эргасистемы

Уровень	Основные функции	Штатные процедуры	Целесообразные методы
7	Информационно-логическая обработка ИМ для решения практических задач Хранение ИМ в архивах и в базе данных и знаний (БДЗ) Выбор средств и передача ИМ. Доступ к БДЗ	— — **1—5, 7, 8, 9**	Оптимизация структур переработки информации. Контроль преобразований. Резервирование и регенерация ИМ. Восстановление ИМ в БДЗ. Отладка и тестирование комплекса программ. НОТ персонала эргасистемы. Физическая изоляция. Профилактика «компьютерных вирусов». Преобразование файлов.
6	Выбор формы представления (*ASCII, EBCDIC* и др.) Сжатие данных (наборов одинаковых кодов) Защитное преобразование	**1**	Защитные преобразования ИМ субъектов
5	Соединение с программой субъекта. Синхронизация служебных ИМ. Обработка приоритетов и прерываний.	—	Идентификация программных компонентов. Автоматическая регистрация прерываний
4	Установление связи по каналу. Установление соответствия между адресами и сетевыми именами абонентов.	**1—4, 7, 9**	
3	Маршрутизация (по адресу) в сети (подсети) эргасистемы.	**1—7, 9**	Реконфигурация подсетей ИРС, адаптивная к отказам и сбоям.
2	Установление связи между соседними информационными узлами. Обнаружение ошибок при передаче данных между соседними узлами.	**1, 9**	
1	Выбор формы сигнала — переносчика ИМ.	**1**	Экранирование кабеля.

иначе возникнет задержка сообщений, которая может привести к блокировке информационного узла (эргасистемы) или существенному снижению его производительности. Это можно обеспечить путем аппаратной реализации алгоритма, что, однако, увеличивает расходы на создание и обслуживание узла.

Сетевой уровень обеспечивает больше услуг по КЗИ, поскольку на нем сосредоточено управление маршрутизацией. Эти услуги обеспечиваются протоколами доступа к подсети, маршрутизации и трансляции. Управление доступом на сетевом уровне позволяет отклонять несанкционированные вызовы и дает возможность различным подсетям управлять использованием ресурсов сетевого уровня.

На *транспортном* уровне осуществляется защита индивидуальных транспортных соединений. На *сеансовом* уровне КЗИ не предусмотрены. На уровне *представления* осуществляется защитное преобразование ИМ ЛВК. *Прикладной* уровень может обеспечить любую услугу по защите информации, хотя некоторые из них обеспечиваются на основе методов, реализуемых на более нижних уровнях. ЛВК сами могут предпринять дополнительные меры по защите своей информации, например, использовать «межоконечное» (*end-to-end)* преобразование на более высоких уровнях.

Выбор и применение других методов и средств КЗИ (см. *табл.*) в сети эргасистемы (на уровне прикладных процессов, на уровнях взаимодействия информационных узлов) должны осуществляться с учетом требований к степени безопасности информации в конкретной сети, структур и принципов оптимизации переработки информации в ИРС эргасистемы[18] [6, 8].

Таким образом, рассмотрена непротиворечивая совокупность и рациональное распределение прагматических методов и целесообразных сетевых аппаратно-программных процедур обеспечения защищенности информации в эргасистемах на основе применения соответствующих принципов контроля и защиты информации от ошибок переработки, разрушающих факторов, несанкционированного доступа и использования.

[18] Ловцов Д. А. Методы защиты информации в АСУ сложными динамическими объектами // НТИ. Сер. 3. Информ. процессы и системы. 2000. № 5. С. 29—45; Защита информации в глобальной сети Интернет // Информатика и образование. 1998. № 5. С. 101—108; Защита информации в информационно-вычислительной сети // НТИ. Сер. 3. Информ. процессы и системы. 1997. № 2. С. 7—13.

Литература

1. Зубов А.Ю. Криптографические методы защиты информации. М. : Гелиос АРВ, 2005. 192 с.
2. Конахович Г.С. Защита информации в телекоммуникационных системах. М. : МК Пресс, 2005. 288 с.
3. Кульба В.В., Ковалевский С.С., Шелков А.Б. Достоверность и сохранность информации в АСУ. М. : Синтег, 2004. 496 с.
4. Ловцов Д.А. Лингвистическое обеспечение правового регулирования информационных отношений в инфосфере. II. Качество информации // Правовая информатика. 2015. № 2. С. 53—61.
5. Ловцов Д.А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. 2017. № 3. С. 66—74.
6. Ловцов Д.А. Информационная теория эргасистем : монография. М. : Росс. гос. ун-т правосудия, 2021. 250 с.
7. Ловцов Д.А. Принципы обеспечения защищенности информации в эргасистемах // Правовая информатика. 2021. № 1. С. 36—50.
8. Ловцов Д.А., Галахова А.Е. Защита интеллектуальной собственности в сети Интернет // Информационное право. 2012. № 4. С. 13—20.
9. Ловцов Д.А., Ермаков И.В. Защита информации от доступа по нетрадиционным информационным каналам // НТИ. Сер. 3. Информ. процессы и системы. 2006. № 9. С. 1—9; Классификация и модели нетрадиционных информационных каналов в эргасистеме // НТИ. Сер. 3. Информ. процессы и системы. 2005. № 3. С. 1—7.
10. Ловцов Д.А., Князев К.В. Защищенная биометрическая идентификация в системах контроля доступа. I. Математические модели и алгоритмы // Информация и космос. 2014. № 2. С. 100—103; II. Качество информационно-математического обеспечения // Информация и космос. 2014. № 3. С. 95—100.
11. Ловцов Д.А., Сухов А.В., Зайцев М.А., Глинский И.В. Информационно-математический подход к киберзащите информационных систем с использованием энтропии покрытия // Вестник Росс. нового ун-та. Сер. «Сложные системы: модели, анализ и управление». 2016. № 1-3. С. 150—157.
12. Ловцов Д.А., Терентьева Л.В. Правовое регулирование международных коммерческих электронных контрактов. Технологические и правовые аспекты электронной подписи // Lex russica. 2020. Т. 73. № 7. С. 115—126.
13. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М. : Академия, 2009. 336 с.
14. Основы технической эксплуатация радиотехнических систем специального назначения / Ратушняк В.Н., Хоменко И.В., Малыков К.А. и др. Под ред. К.А. Малыкова. Красноярск : Сиб. фед. ун-т, 2015. 335 с.
15. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты. СПб. : Питер, 2008. 272 с.
16. Солодовников В.И. Регистры сдвига и криптоалгоритмы на их основе. Берлин : LAP LAMBERT Academic Publishing, 2017. 112 с.
17. Файтс Ф., Джонстон П., Кратц М. Компьютерный вирус: проблемы и прогноз. М. : Мир, 2013. 176 с.
18. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М. : ДМК Пресс, 2008. 544 с.
19. Шнайер Б. Прикладная криптография. М. : Триумф, 2013. 518 с.

Рецензент: ***Цимбал Владимир Анатольевич,*** *доктор технических наук, профессор, заслуженный деятель науки РФ, профессор кафедры автоматизированных систем боевого управления Филиала Военной академии им. Петра Великого, г. Серпухов.*
E-mail: tsimbalva@mail.ru

METHODS AND PROCEDURES FOR ENSURING INFORMATION SECURITY IN ERGASYSTEMS

Dmitrii Lovtsov, *Dr.Sc. (Technology), Professor, Meritorious Scientist of the Russian Federation, Deputy Director for Research of Lebedev Institute of Precision Mechanics and Computer Engineering of the Russian Academy of Sciences, Head of the Department of Information Technology Law, Informatics and Mathematics of the Russian State University of Justice, Moscow, Russian Federation.*
E-mail: dal-1206@mail.ru

Keywords: *ergasystem, information security, reliability, confidentiality, integrity, methods of ensuring, hardware and software procedures, information distribution network, pragmatic classification, indicators, criteria, information control and protection subsystem, organisational and functional principles.*

Abstract.

Purpose of the paper: improving the scientific and methodological basis of the theory of information security in ergasystems.

Methods used: system analysis, complex task formalisation, pragmatic classification and distribution of the basic methods and hardware and software procedures for ensuring information security in ergasystems.

Results obtained: the mathematical structure of the multi-faceted task of ensuring information security in ergasystems was determined. The logical sequence of methodological stages of development of the information control and protection subsystem based on pragmatic organisational and functional principles was determined. A justification was given for a noncontradictory corpus of methods of information control and protection against processing errors, destructive factors, and unauthorised access and use. A justification was given for a pragmatic classification of the basic methods and a distribution of appropriate hardware and software procedures for ensuring information security in ergasystems.

The obtained results are a conceptual and theoretical foundation for setting up efficient information and mathematical support for information control and protection in ergasystems.

References

1. Zubov A.Iu. Kriptograficheskie metody zashchity informatsii. M. : Gelios ARV, 2005. 192 pp.
2. Konakhovich G.S. Zashchita informatsii v telekommunikatsionnykh sistemakh. M. : MK Press, 2005. 288 pp.
3. Kul'ba V.V., Kovalevskii S.S., Shelkov A.B. Dostovernost' i sokhrannost' informatsii v ASU. M. : Sinteg, 2004. 496 pp.
4. Lovtsov D.A. Lingvisticheskoe obespechenie pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere. II. Kachestvo informatsii. Pravovaia informatika, 2015, No. 2, pp. 53-61.
5. Lovtsov D.A. Problema garantirovannogo obespecheniia informatsionnoi bezopasnosti krupnomasshtabnykh avtomatizirovannykh sistem. Pravovaia informatika, 2017, No. 3, pp. 66-74.
6. Lovtsov D.A. Informatsionnaia teoriia ergasistem : monografiia. M. : Ross. gos. un-t pravosudiia, 2021. 250 pp.
7. Lovtsov D.A. Printsipy obespecheniia zashchishchennosti informatsii v ergasistemakh. Pravovaia informatika, 2021, No. 1, pp. 36-50.
8. Lovtsov D.A., Galakhova A.E. Zashchita intellektual'noi sobstvennosti v seti Internet. Informatsionnoe pravo, 2012, No. 4, pp. 13-20.
9. Lovtsov D.A., Ermakov I.V. Zashchita informatsii ot dostupa po netraditsionnym informatsionnym kanalam. NTI, ser. 3, Inform. protsessy i sistemy, 2006, No. 9, pp. 1-9; Klassifikatsiia i modeli netraditsionnykh informatsionnykh kanalov v ergasisteme. NTI, ser. 3, Inform. protsessy i sistemy, 2005, No. 3, pp. 1-7.
10. Lovtsov D.A., Kniazev K.V. Zashchishchennaia biometricheskaia identifikatsiia v sistemakh kontrolia dostupa. I. Matematicheskie modeli i algoritmy. Informatsiia i kosmos, 2014, No. 2, pp. 100-103; II. Kachestvo informatsionno-matematicheskogo obespecheniia. Informatsiia i kosmos, 2014, No. 3, pp. 95-100.
11. Lovtsov D.A., Sukhov A.V., Zaitsev M.A., Glinskii I.V. Informatsionno-matematicheskii podkhod k kiberzashchite informatsionnykh sistem s ispol'zovaniem entropii pokrytiia. Vestnik Ross. novogo un-ta. Ser. "Slozhnye sistemy: modeli, analiz i upravlenie", 2016, No. 1-3, pp. 150-157.
12. Lovtsov D.A., Terent'eva L.V. Pravovoe regulirovanie mezhdunarodnykh kommercheskikh elektronnykh kontraktov. Tekhnologicheskie i pravovye aspekty elektronnoi podpisi. Lex russica, 2020, t. 73, No. 7, pp. 115-126.
13. Mel'nikov V.P., Kleimenov S.A., Petrakov A.M. Informatsionnaia bezopasnost' i zashchita informatsii. M. : Akademiia, 2009. 336 pp.
14. Osnovy tekhnicheskoi ekspluatatsiia radiotekhnicheskikh sistem spetsial'nogo naznacheniia. Ratushniak V.N., Khomenko I.V., Malykov K.A. i dr. Pod red. K.A. Malykova. Krasnoiarsk : Sib. fed. un-t, 2015. 335 pp.
15. Rodichev Iu.A. Informatsionnaia bezopasnost': normativno-pravovye aspekty. SPb. : Piter, 2008. 272 pp.
16. Solodovnikov V.I. Registry sdviga i kriptoalgoritmy na ikh osnove. Berlin : LAP LAMBERT Academic Publishing, 2017. 112 pp.
17. Faits F., Dzhonston P., Kratts M. Komp'iuternyi virus: problemy i prognoz. M. : Mir, 2013. 176 pp.
18. Shan'gin V. F. Zashchita komp'iuternoi informatsii. Effektivnye metody i sredstva. M. : DMK Press, 2008. 544 pp.
19. Shnaier B. Prikladnaia kriptografiia. M. : Triumf, 2013. 518 pp.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, РЕАЛИЗУЮЩЕЕ АЛГОРИТМ ШАМИРА В СТОЙКИХ ЧАСТНЫХ КРИПТОСИСТЕМАХ

*Гриднев В.А., Селиванов А.Ю.**

***Ключевые слова**: программное обеспечение, криптосистема, ключ шифрования, депонирование, пороговая схема разделения секрета, алгоритм, контроль аутентичности теней, безопасность, информационная система, пользователь.*

Аннотация.

Цели работы: облегчение работы пользователя при разделении секрета на основе прикладного программного обеспечения, реализующего систему депонирования ключей шифрования в стойких частных криптосистемах, использующих пороговую схему Шамира.

Методы: объектно-ориентированное программирование, имитационное моделирование.

Результаты: обоснована необходимость применения стойких частных криптосистем с депонированием ключей; приведены актуальные примеры использования таких систем; разработан программный комплекс для депонирования ключей на основе пороговой схемы Шамира; исследованы правовые вопросы депонирования ключей в частных криптосистемах.

Программный комплекс включает программу, предоставляющую простой интерфейс разделения и восстановления секрета, а также программу, встраиваемую в стороннее программное обеспечение в виде заголовочной библиотеки. Главной особенностью программного комплекса является простота, его использование не требует особой квалификации.

DOI: 10.21681/1994-1404-2021-3-50-59

Введение

В современном мире все более актуальными становятся проблемы цифровых преступлений и международного терроризма. В условиях тотальной распространенности доступа в сеть Интернет и развития общедоступных систем шифрования цифровое общение злоумышленников становится все труднее отслеживать [8]. В связи с этим проведено исследование эффективности применения пороговых схем разделения секрета на основе депонирования ключей шифрования [4, 11].

Депонирование ключей — это предоставление ключей шифрования или их частей (*теней*) третьей стороне[1]. Третья сторона имеет право использовать тени или ключи лишь при определенных обстоятельствах, в частном случае, по решению суда. Как правило, третьей стороной выступают государственные организации и правоохранительные органы. Конечно же, депонирование секрета — это сложная с этической точки зрения задача, часто граждане не хотят добровольно «делиться» секретом или его частями из-за вполне оправданных мыслей о слежке.

Данное исследование, помимо создания программного обеспечения для разделения секрета, имеет целью привести примеры разрешения названной сложной задачи.

Процедуры разделения ключей

Криптосистемы с депонированием ключей. Анализ показал, что депонирование ключей необходимо для обеспечения баланса между тайной личной переписки граждан и полной криптоанархией, позволяющей криминальным элементам безопасно общаться по

[1] *Shamir A. How to share a secret*. 1979. *Communications of the ACM* 22. P. 612-613.

* ***Гриднев Виктор Алексеевич,*** *кандидат технических наук, доцент, доцент кафедры информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*
E-mail: vikadres@yandex.ru

Селиванов Александр Юрьевич, *студент 5 курса Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*
E-mail: istrebion@yandex.ru

открытым каналам связи, используя стойкое шифрование, таким образом угрожая интересам национальной безопасности.

В США начиная с 1992 г. были попытки депонировать ключ, используемый для шифрования данных, передаваемых по каналам *Integrated Services Digital Network*, факсам и любой связи того времени [4]. Для этого был разработан стандарт — *Escrowed Encryption Standard*[2]. Реализованы эти попытки были при помощи микросхемы *Clipper*, занимающейся шифрованием и расшифровкой данных. Агентство национальной безопасности США (*NSA*) также разработало дисциплину раскрытия уникального ключа микросхемы. Микросхема была разработана по технологии *Tempest* таким образом, чтобы было невозможно считать с нее данные по каналам побочных электромагнитных излучений и наводок.

Простейший пример схемы разделения секрета. Допустим, имеется тайное общество, строящее планы по захвату мира, которое состоит из N человек. Члены общества создали сообщение s, состоящее из бинарных символов. Затем они случайным образом подобрали N значений двоичных сообщений таким образом, что в сумме они давали изначальное сообщение s. Теперь, если все члены общества соберутся вместе, они без труда смогут подтвердить свое членство, просто сложив все N сообщений вместе. Если в итоге получится изначальное сообщение s, известное всем, то общество собралось в полном составе. В противном же случае — в общество пробрался «обманщик». У данной схемы есть множество проблем, но самая серьезная состоит в том, что если хотя бы один член группы захочет выйти из нее, то придется менять все N двоичных сообщений. Более того, если на сбор группы не придет хотя бы один из ее участников, подтвердить подлинность членов тайного общества не получится.

Существует более продуманная схема разделения секрета, позволяющая подтверждать подлинность участников нашего мнимого тайного общества, даже если оно не собирается в полном составе. Называется данная схема *пороговой*. Первые идеи схем, в которых число теней, необходимых для восстановления секрета, не равно числу участников (t и n, соответственно) принадлежат известному криптографу Ади Шамиру, одному из авторов известного алгоритма *RSA*.

Пороговая схема. Если собравшееся число участников таково, что возможно восстановление секрета, такую коалицию называют *разрешенной*. Следует заметить, что пороговые схемы, в которых разрешенные группы участников, имеющие число теней, равное или большее числу теней, необходимых для восстановления секрета, всегда могут однозначно восстановить зашифрованный ранее секрет, а неразрешенные не получают никакой информации о возможном значении секрета, называют *совершенными*[3].

Схема Шамира. Перейдем к конкретным примерам схем, которые могли бы использовать члены нашего гипотетического тайного общества. Основная идея состоит в том, что в геометрии двумерного пространства по двум точкам можно построить прямую, по трем параболу, по четырем кубическую параболу и так далее, повышая степени. Иными словами, для задания степенного многочлена k требуется число точек, равное $(k + 1)$[4].

Для того чтобы восстановить секрет могло только определенное число членов тайного общества n, секрет сворачивают в многочлен степени $n + 1$ над конечным полем G. Таким образом, чтобы восстановить секрет, необходимо будет собрать вместе n членов тайного общества, а значит, и значений многочлена в определенных точках. Если тайное общество не сможет собраться в нужном количестве, точек будет недостаточно, и восстановление секрета будет невозможно. В теории, число точек многочлена не ограничено, но ввиду конечности памяти ЭВМ и разумной достаточности (в нашей организации вряд ли будет большее число членов чем, к примеру, миллион) оно всегда ограничено размерностью поля Галуа порядка G.

Попробуем описать алгоритм более кратко. Допустим, мы имеем поле Галуа G. Возьмем n случайных элементов данного поля, обладающих свойством дискретности и не попадающих в ноль. Выберем произвольный набор элементов t поля Галуа G. Число элементов набора будет необходимым для восстановления секрета. Именно из этого множества чисел будет составляться искомый *пороговый* многочлен над полем Галуа степени $(t — 1)$, $1 < t \leq n$.

Допустим, искомый многочлен получен, теперь найдем его значения (x, y) в n точках. Остается лишь распределить полученные значения каждому из членов нашего тайного общества.

Заметим, что через две точки всегда можно провести неограниченное число квадратичных парабол (*рис*. 1). Но чтобы выбрать из них нужную параболу, понадобится третья точка.

Восстановление секрета осуществляется с помощью любой формулы интерполяции, например, при помощи наиболее популярной формулы Ньютона или Бесселя.

Основное достоинство пороговой схемы Шамира — масштабируемость. Если в нашем тайном сообществе появится новый участник, то нам будет необходимо добавить новый несекретный элемент к уже созданным ранее несекретным элементам. Если же, наоборот, какой-либо член нашего сообщества был исключен, то это не приводит к необходимости генерации нового

[2] Блэкли Д., Кабатянский Г. А. Обобщенные идеальные схемы, разделяющие секрет, и матроиды // Пробл. передачи информ. 1997. Т. 33. Вып. 3. С. 102—110.

[3] Блейхут Р. Теория и практика кодов, контролирующих ошибки (*Theory and Practice of Error Control Codes*). М. : Мир, 1986. 576 с.

[4] Ященко В. В., Варновский Н. П., Нестеренко Ю. В. Введение в криптографию. М. : МЦНМО «ЧеРо», 1999. 272 с.

набора точек. По сути, это просто ослабит схему, переведя ее из (n, t)-пороговой в $(n — 1, t — 1)$-пороговую.

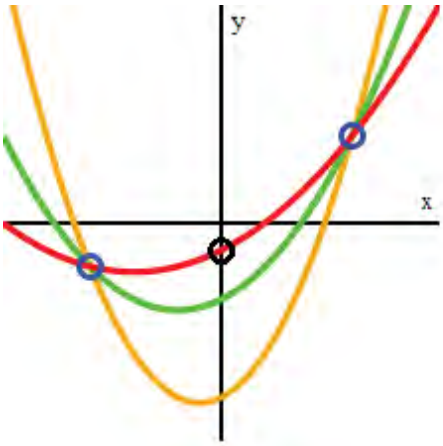

Рис. 1. Квадратичные параболы

Схема Блэкли. Какие еще варианты могут быть у нашей мнимой тайной организации? Известным фактом является то, что две непараллельные прямые на плоскости всегда пересекаются в одной точке. Таким образом, две некомпланарные плоскости всегда пересекаются по одной прямой, соответственно, три некомпланарные плоскости всегда пересекаются в одной точке. Более того, *n n*-мерных гиперплоскостей всегда пересекаются в одной точке (*рис*. 2).

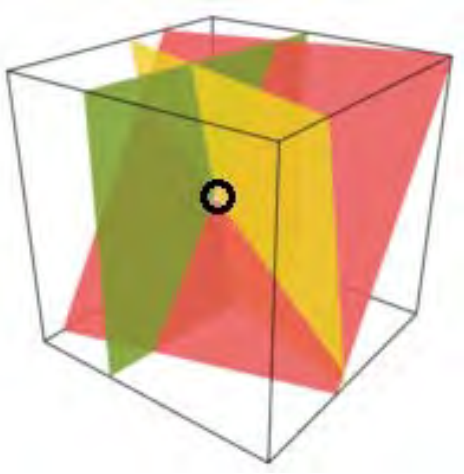

Рис. 2. Пересечение гиперплоскостей

Основная идея состоит в том, что одна из координат этой точки пересечения будет являться секретом [17].

Если мы закодируем секрет как несколько координат точки, то восстановление части секрета будет возможно уже по одной доле секрета, в более широком смысле — по одной гиперплоскости. Секретом здесь, в математическом смысле, будет являться взаимосвязанность координат точки пересечения [15].

Таким образом, с помощью схемы Блэкли мы сможем создать (t, n)-пороговую схему разделения секрета для любых t и n. Для этого придется использовать большие размерности пространства t. Каждому из n членов нашего сообщества необходимо будет выдать одну гиперплоскость, проходящую через точку, которая и будет являться секретом. Тогда любые t из общего числа n гиперплоскостей будут однозначно пересекаться в секретной точке.

Из всего сказанного можно сделать вывод, что схема Блэкли значительно менее эффективна, чем схема Шамира. Дело в том, что в схеме Шамира каждая тень того же размера, что и секрет. Размер тени имеет вполне практическое значение, ведь чем тень короче, тем проще ее запомнить. В схеме Блэкли каждая доля больше секрета в число раз, равное числу теней, необходимых для восстановления секрета. Более того, схема Блэкли не обладает такой же гибкостью, что и схема Шамира [2].

Существуют улучшения схемы Блэкли, позволяющие понизить ее ресурсоемкость и повысить гибкость, но, к сожалению, все они сильно усложняются по сравнению со схемой Шамира[5].

Схемы, основанные на решении систем уравнений. Математикам давно известно, что не существует решений систем линейных алгебраических уравнений (СЛАУ), в которых число уравнений меньше, чем число неизвестных.

Возьмем $n+1$ m-мерных векторов $V_0, V_1, \ldots V_n$ таким образом, чтобы квадратная матрица размера m, составленная из выбранных векторов, имела ранг m. Пусть выбранный вектор U имеет размер m, тогда секретом в нашей схеме будет матричное произведение транспонированного вектора U на другой выбранный ранее вектор V_i. Таким образом, долями секрета будут произведения транспонированного вектора U на V_i, где $i = 0, \ldots, n$[6].

Заметим, что по любым m долям можно составить СЛАУ размерности m, неизвестными в которой являются коэффициенты вектора U. Решив данную систему, можно найти коэффициенты U, а имея их, можно найти и секрет. При этом, естественно, СЛАУ неразрешима, если число неизвестных будет больше числа уравнений, т. е. если число долей меньше m [13].

Данный принцип реализован в схеме Карнина-Грина-Хеллмана [14].

Из-за хорошей способности к масштабируемости и отсутствия нелинейного роста алгоритмической сложности в схеме разделения секрета по Шамиру выбор авторов пал именно на нее.

Разработка программного обеспечения

Главной целью разработки программного комплекса была реализация лучшего способа разделения и восстановления ключа шифрования без усложнения алгоритма контролем законности операции восстановления и легитимности уполномоченного субъекта. Раз-

[5] Blakley G. R. Safeguarding cryptographic keys. Proceedings of the National Computer Conference, 48, 1979. P. 313-317.

[6] Karnin E. D., Greene J. W., Hellman M. E. On Secret Sharing Systems. F. Kschischang, IEEE, 1983. Vol. 29, Iss. 1. P. 35-41.

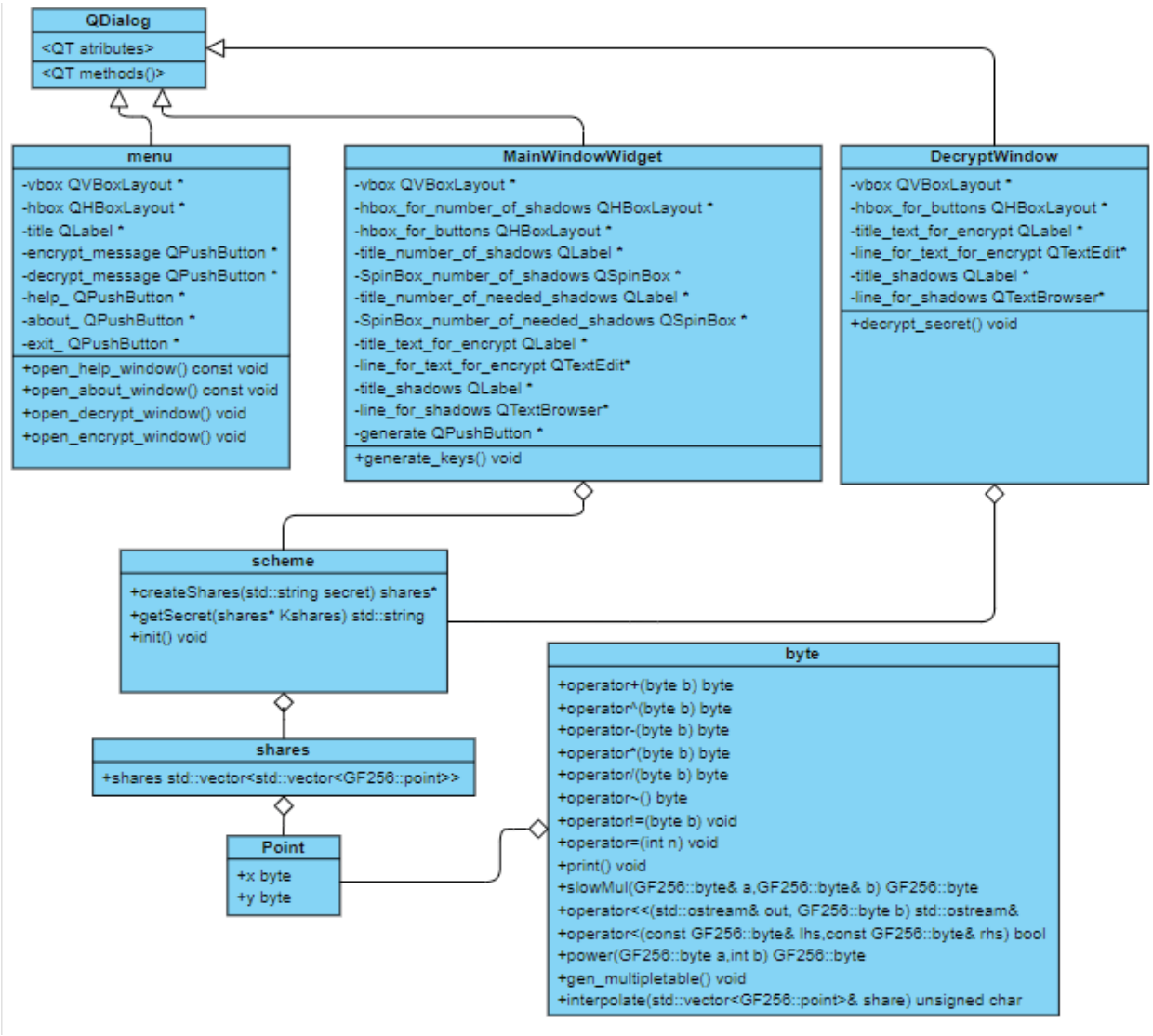

Рис. 3. Диаграмма классов программного комплекса

работанный программный комплекс использует простую пороговую схему, так что необходимо однократно потратить около двух-трех минут на разделение ключа. Ключи необходимо разделять один раз за срок их действия (около одного года). Конечно же, пороговые схемы сто́ит использовать в комплексе с уже готовыми приложениями для передачи информации. К примеру, вместе с любым известным мессенджером.

Программу, реализующую разделение секрета, можно оформить в виде небольшого кроссплатформенного модуля, который с легкостью можно будет интегрировать в любой сервис генерации ключей шифрования независимо от используемого языка программирования. Модули, реализующие разделение и восстановление секрета, должны быть оформлены раздельно, так как они выполняются на разных устройствах. При этом демонстрационную программу можно выполнить в виде единого модуля, реализующего все функции для имитационного моделирования.

Язык и инструментальные средства программирования. В качестве языка программирования для реализации программного обеспечения (ПО), был выбран язык *C++*. Это популярный компилируемый язык со статической типизацией [5]. Выбранный язык является достаточно низкоуровневым для решения с его помощью криптографических задач. Приложение было написано с использованием объектно-ориентированного подхода, что позволило придать архитектуре высокую скорость выполнения, гибкость и масштабируемость. Заметим, что в состав языка C++ включена библиотека *STL*. В данный набор шаблонов включена бóльшая часть контейнеров для работы с памятью, а также множество алгоритмов.

Программа была собрана при помощи компилятора *MinGW*; несмотря на то, что это компилятор для *Windows*, написанный код может использоваться и для других платформ, используя другие компиляторы.

В качестве инструментальных средств программирования была выбрана программная среда *QTCreator*, поддерживающая графический интерфейс.

Описание программного комплекса. Программный комплекс *ShamirSecretDepoKeys.exe* предназначен для

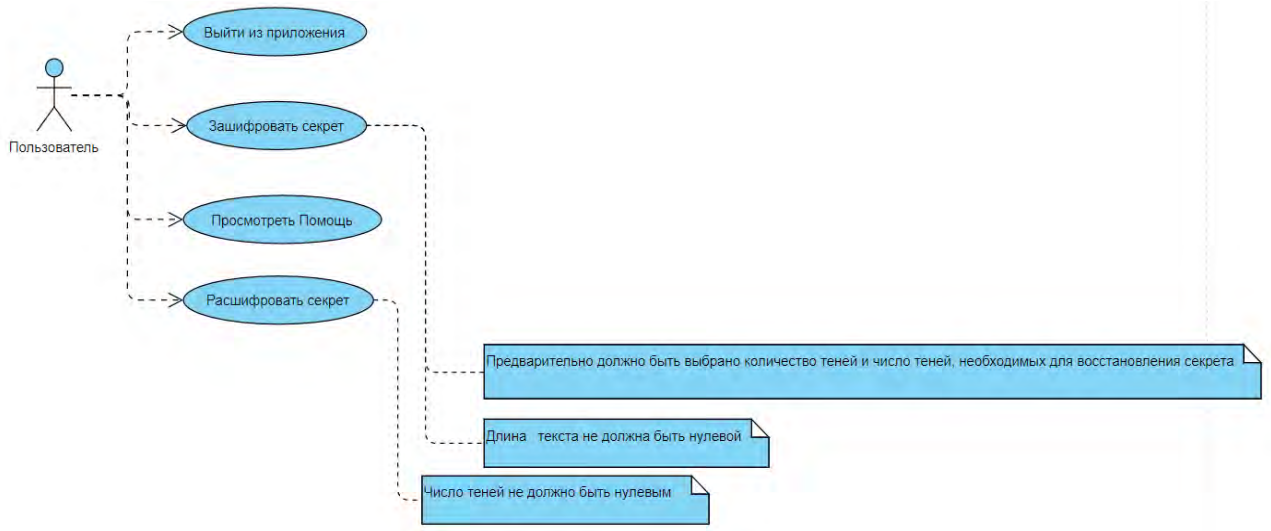

Рис. 4. Диаграмма вариантов использования программного комплекса

разделения и восстановления секрета по схеме Шамира. Данная программа написана на языке *C++* с использованием интегрированной среды разработки *QtCreator*.

Программный комплекс имеет модульную архитектуру и содержит 13 программных модулей:

– файлы исходного кода: shamir.cpp, menu.cpp, mainwindowwidget.cpp, main.cpp, GF(256).cpp, decryptwindow.cpp.;
– заголовочные файлы: shamir.h, mainwindowwidget.h, main.h, GF(256).h, decryptwindow.h, menu.h.;
– файл проекта: ShamirSecretDepoKeys.pro.

Модули *mainwindowwidget.h, menu.h, decryptwindow.h, decryptwindow.cpp, menu.cpp, mainwindowwidget.cpp* нужны для обеспечения логики содержимого окон графического интерфейса. Модули *shamir.h, shamir.cpp, main.h, GF(256).h, GF(256).cpp* предназначены для описания логики разделения и восстановления секрета.

Архитектура ПО обладает достаточной гибкостью и масштабируемостью.

Диаграмма классов и диаграмма вариантов использования. Диаграмма классов (от англ. *class diagram*) — это диаграмма языка *UML*, показывающая структуру классов программы. Данная диаграмма описывает поля и методы классов, типы возвращаемых значений, структуру наследований и интерфейсов [3]. Применяется не только для визуализации, но и для прямого или обратного планирования архитектуры. Авторы использовали данную диаграмму именно для прямого планирования архитектуры программного комплекса (*рис.* 3). Диаграмма вариантов использования (от англ. *use case diagram*) в *UML* — это диаграмма, отражающая отношения между акторами и прецедентами и являющаяся составной частью модели прецедентов, позволяющей описать систему на концептуальном уровне [6]. Диаграмма прецедентов разработанного ПО показана на *рис.* 4.

Рис. 5. Основное окно интерфейса программного комплекса

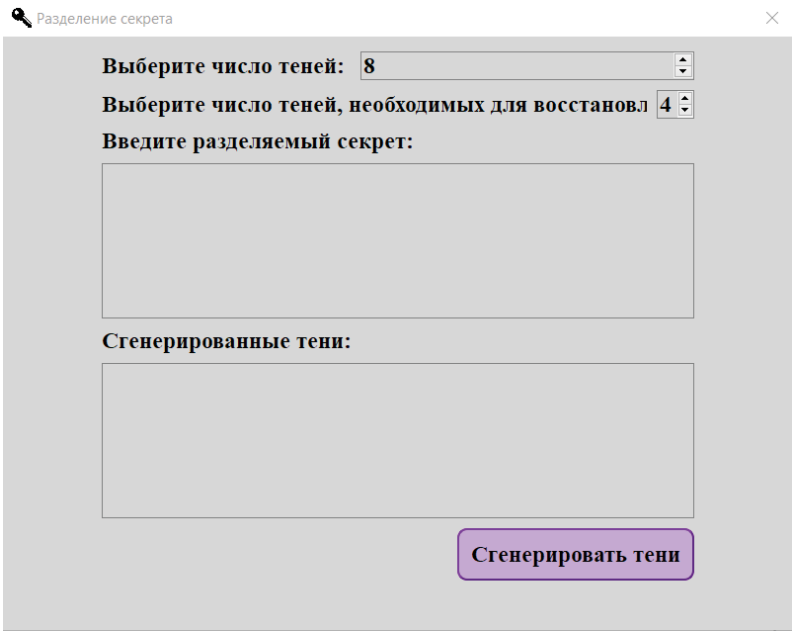

Рис. 6. Окно интерфейса «Шифрование секрета»

Интерфейс программного комплекса. Вид основного окна программного комплекса представлен на *рис*. 5.

На *рис*. 6 показан вид окна интерфейса «Разделение секрета». В этом окне пользователь может разделить секрет на тени, выбрав общее число теней и число теней, необходимых для восстановления секрета. Программа позволяет выбирать число теней в диапазоне от 5 до 10 единиц. Допустимый диапазон числа теней, необходимых для восстановления, находится в диапазоне от 2 до 5. Это сделано в интересах моделирования. Реальные схемы целесообразно сделать двух видов: 2 из 4 и 3 из 5.

Сгенерируем ключ шифрования длиной 256 *бит* и попробуем зашифровать секретную фразу «*Sapere aude*!» алгоритмом *AES* с помощью сгенерированного ключа (*рис*. 7).

Следующий пример доказывает эффективность программного комплекса разделения закрытого ключа:

"*AADRkK7s32waZoO2d/IvDejqbWEZa8L2*",

выбрав общее число теней 8, а число теней, необходимых для восстановления секрета — 4. Такая пороговая схема называется (4, 8).

Результат генерации теней показан на *рис*. 8. Рассмотрим конкретную тень: 8 1 114 198 103 46 157 156 118 227 93 65 210 140 43 122 42 14 7 58 41 206 94 82 241 99 34 242 128 155 64 139 191 101. *Первое* число означает общее количество теней в пороговой схеме, *второе* число — номер конкретной тени. Все дальнейшие числа являются, собственно, тенью.

На *рис*. 9 показано окно интерфейса «Восстановление секрета». В данном окне пользователь вводит тени, разделяя их знаком новой строки. Если какая-то из теней повреждена или число теней меньше ранее заданного количества, восстановления секрета не произойдет.

Как видно, ключ был успешно восстановлен по четырем теням из восьми. Проверим результат восстановления ключа, расшифровав исходное сообщение (*рис*. 10).

На *рис*. 11 приведен пример окна интерфейса «Помощь».

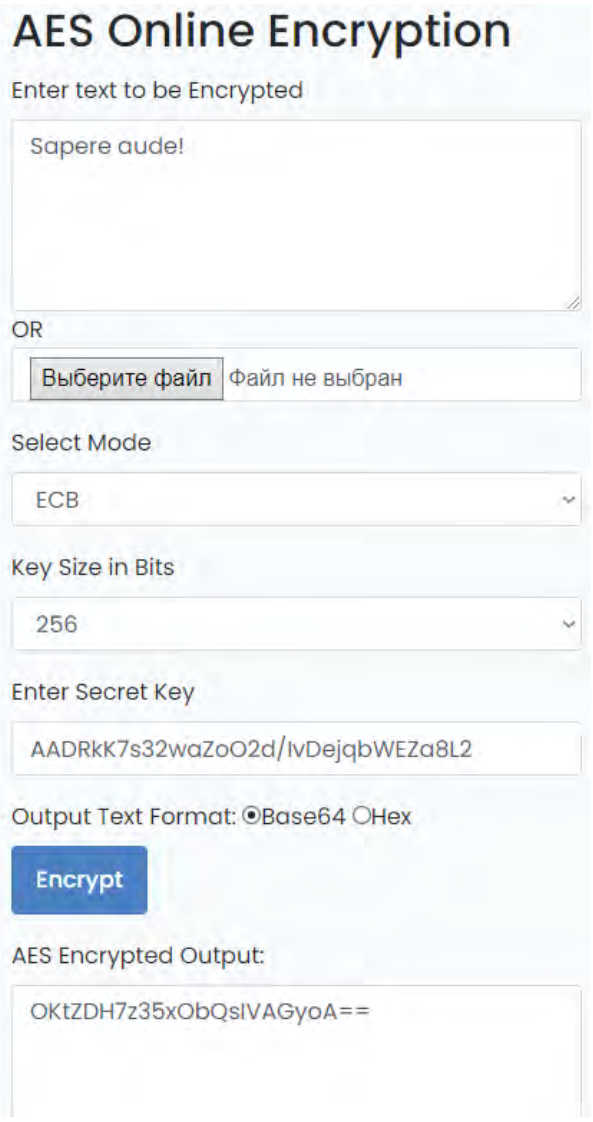

Рис. 7. Шифрование сообщения

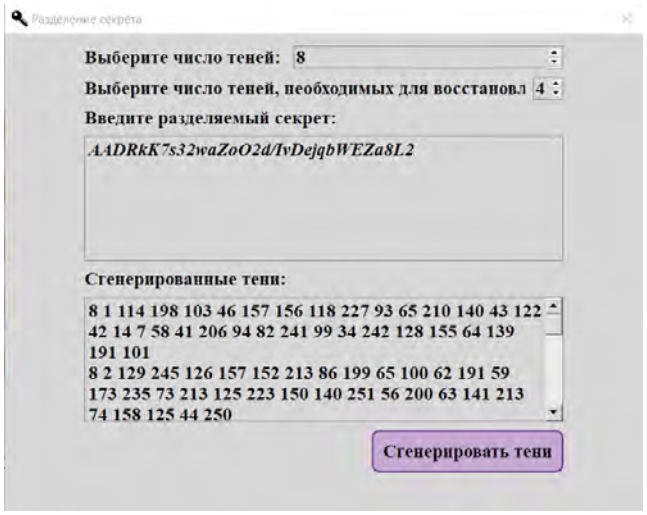

Рис. 8. Результат генерации теней

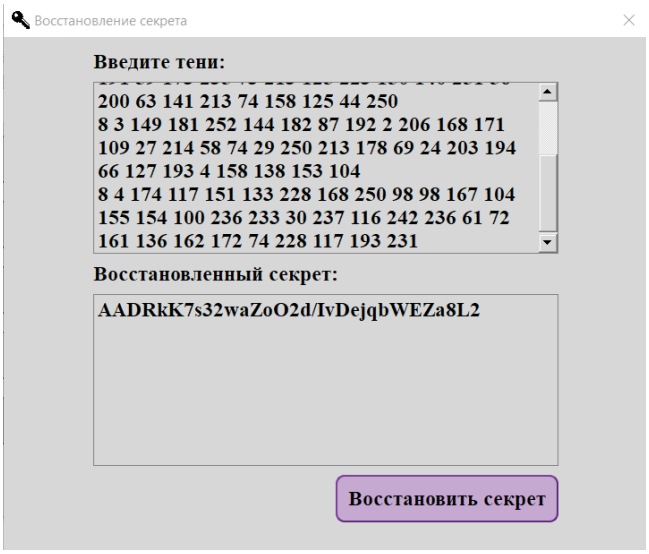

Рис. 9. Интерфейс окна «Восстановление секрета»

Как видно, восстановление секретной фразы произошло корректно.

Примеры применения разработанного программного комплекса

Депонирование ключей с целью обеспечения безопасности граждан. В настоящее время распространение получили криптографические алгоритмы, позволяющие обеспечить такой уровень криптостойкости, который не под силу взломать спецслужбам разных стран. Это создает определенные проблемы в таких сферах, как борьба с мировым терроризмом. Решение данных проблем — этически сложная задача, поскольку необходимо сохранять секретность переписки, давая разрешение спецслужбам на ее чтение лишь при наличии веских улик. Но как заставить пользователей системы добровольно передать тени ключей в центр хранения теней? Данная задача должна решаться с помощью механизма запрета использования определенной информационной системы пользователям, не передавшим тени центру хранения теней [12].

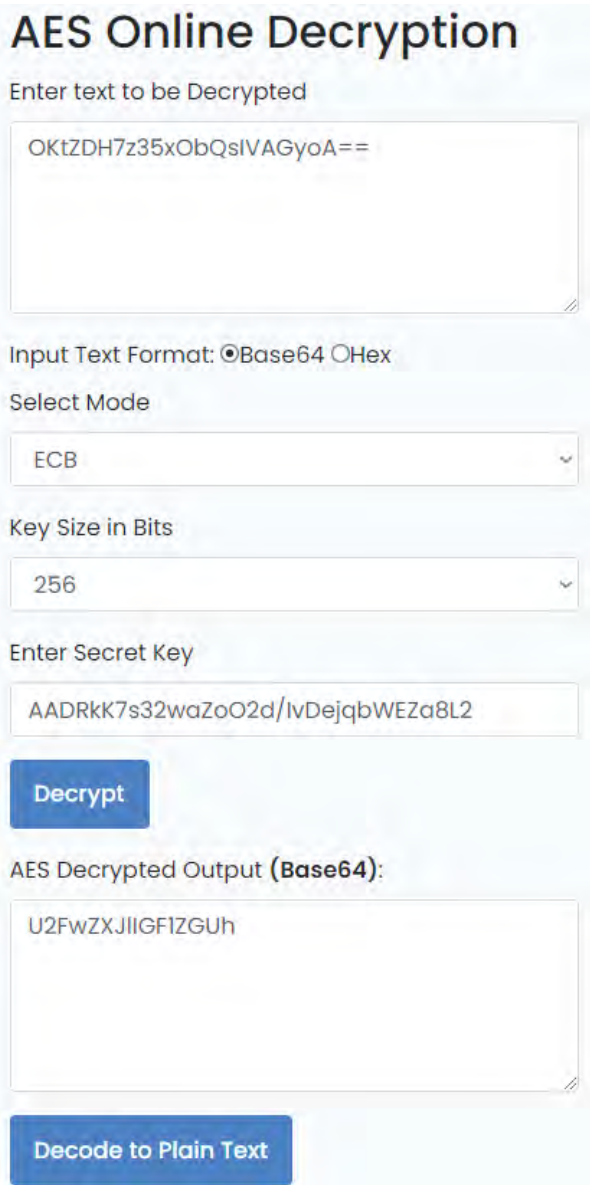

Рис. 10. Восстановление секретной фразы

К примеру, определенный пользователь хочет использовать информационную систему (в частном случае — мобильное приложение) со стойким шифрованием. При регистрации пользователь дает свое согласие на депонирование теней ключа шифрования и их распределение по центрам хранения теней. В противном случае пользователь не сможет воспользоваться информационной системой.

Пользователя необходимо также уведомить, что за попытку передачи ложных теней ключа его ждет ответственность, а также уверить в том, что ключ не будет восстановлен без соответствующего решения суда. Увеличение числа теней ключа увеличивает стойкость системы в целом, так как условному нарушителю будет необходимо украсть большее число теней, проникнув в соответственно большее число информационных систем. Определенная часть пользователей информационных систем может радикально выступать против передачи теней в государственные центры хранения.

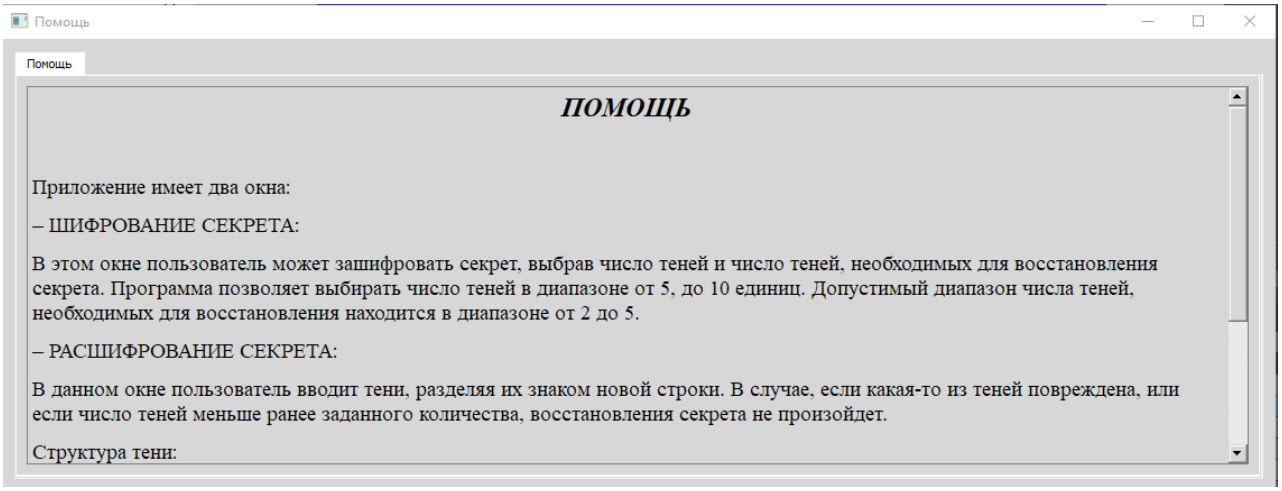

Рис. 11. Окно интерфейса «Помощь»

Для купирования данного эффекта стоит передавать тени «скрытно», обязательно указав все условия в лицензионном соглашении[7] [17].

Депонирование с целью восстановления ключа при его утрате. В последние годы все большую популярность набирают различные криптовалюты, основанные на системе блокчейна [8, 9]. Криптовалюты по сути своей являются децентрализованными. В случае потери доступа к банковскому счету пользователь банка пишет запрос в филиал, подтверждает свою личность, после чего банк восстанавливает доступ.

В случае криптовалют при потере доступа к кошельку средства, содержащиеся на нем, будут утеряны навсегда. Таким образом, пользователь сам заинтересован в раздельном сохранении теней секрета, чтобы не потерять доступ к криптовалюте, например, при повреждении оборудования, на котором хранится ключ. Пороговая схема разделения секрета Шамира позволит обеспечить безопасное раздельное хранение [16]. Если какой-либо центр хранения потеряет ключ или будет взломан, это не приведет к негативным последствиям для пользователей.

Данная идея может позволить вывести криптовалюты из теневой части рынка, введя их в правовое поле. Необходимо лишь создать соответствующие *правовые регламенты* [7, 8], которые не позволят использовать криптовалюты без выдачи теней государственным центрам хранения.

Эта схема может также использоваться для «холодного» хранения теней на внешних носителях данных, таких, как оптические диски. Это позволит восстановить секрет даже при повреждении или утере части накопителей.

Заключение

Решение проблемы депонирования ключей — этически сложная задача, поскольку необходимо сохранять секретность переписки, давая разрешение спецслужбам на ее чтение лишь при наличии веских причин, подтвержденных решением суда. Тем не менее депонирование может использоваться не только для обеспечения возможности чтения личной переписки спецслужбами, но и обеспечения безопасности криптовалют.

Авторы статьи выступают за свободу Интернета, но свобода возможна лишь в правовых рамках, иначе эта свобода превратится в криптоанархию.

Еще в 1997 г. известный криптограф Б. Шнайер четко указал на то, что государственные системы шифрования не получат широкого распространения в будущем [14]. Тем не менее депонирование ключей возможно осуществить, если оно будет выгодно самому пользователю. Более того, весь мир движется в сторону контроля Интернета, и Россия не станет исключением ввиду вступления в силу «закона Яровой» 2016 г. На текущий момент контроль информационного поля — решенный вопрос, осталось лишь выбрать методы. Одним из вариантов данного контроля является расширение «закона Яровой», обязующее владельцев информационных систем обмена сообщениями передавать тени ключей в государственные центры хранения. В случае невыполнения данных требований в законе сто́ит четко прописать размер санкций.

Сто́ит добавить, что весь информационный обмен между субъектами взаимоотношений, приведенных в примерах использования депонирования ключей, может быть реализован в электронном виде, что неизбежно потребует принятия мер по обеспечению безопасности информации, передаваемой по каналам связи [1, 10].

Актуальным остается вопрос защиты *целостности* и *корректности* депонируемых теней. Необходимо предусмотреть защиту депонируемых теней от умышленного или случайного искажения, а также возможность обнаружить любого недобросовестного участника схемы. Ведь любой из участников схемы может попытаться помешать успешному восстановлению ключа. Например, пользователь может после депонирования ключа шифрования использовать совсем другой ключ. И когда после соблюдения всех предусмотренных фор-

[7] B. McCullough, "The NSA tried this before — what the 90s debate over the clipper chip can teach us about digital privacy". Internet History Podcast, URL: http://www.internethistorypodcast.com/2014/08/the-nsa-tried-this-before-what-the-90s-debate-over-the-clipper-chip-can-teach-us-about-digital-privacy-debates/ (дата обращения: 09.05.2021).

мальностей ключ не восстановится, заявить, что он не знает причину, по которой это могло произойти.

Необходимо также предусмотреть электронное взаимодействие всех участников схемы, исключающее необходимость личных встреч и долгого ожидания. Получение ключа шифрования пользователем, депонирование теней, обращение в суд за разрешением на восстановление ключа и само восстановление ключа шифрования сотрудником спецслужб должны происходить путем сетевого электронного взаимодействия.

Литература

1. Алексеев В.В., Стрельцов А.А., Емельянов Е.В. Правовой подход к построению защиты информации в организации // Правовая информатика. 2020. № 2. С. 54—61. DOI: 10.21681/1994-1404-2020-2-54-61 .
2. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. М. : КомКнига, 2006. 328 с.
3. Буч Г., Рамбо Дж., Джекобсон А. Язык UML. Руководство пользователя. 2-е изд. СПб. : ДМК Пресс, 2004. 432 с.
4. Гриднев В.А., Володин И.С., Желудкова А.М. Организационно-правовые вопросы внедрения стойких частных криптосистем // Правовая информатика. 2021. № 1. С. 51—60. DOI: 10.21681/1994-1404-2021-1-51-60 .
5. Керниган Б.У., Ритчи Д.М. Язык программирования С. М. : Вильямс, 2009. 304 с.
6. Ларман К. Применение UML 2.0 и шаблонов проектирования. 3-е изд. М. : Вильямс, 2006. 736 с.
7. Ловцов Д.А. Системология правового регулирования информационных отношений в инфосфере : монография. М.: РГУП, 2016. 316 с. ISBN 978-5-93916-505-1.
8. Ловцов Д.А. Информационно-правовые основы правоприменения в цифровой сфере // Мониторинг правоприменения. 2020. № 2(35). С. 44—52. DOI: 10.21681/2226-0692-2020-2-44-52 .
9. Ловцов Д.А. Информационная безопасность автоматизированных блокчейн-систем: угрозы и способы повышения // Тр. II Междунар. науч.-прак. конф. «Трансформация национальной социально-экономической системы России» (22 ноября 2019 г.) / РГУП. М. : РГУП, 2020. С. 464—473. ISBN 978-5-93916-823-6.
10. Ловцов Д.А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. 2017. № 3. С. 66—74. DOI: 10.21681/2226-0692-2017-3-66-74 .
11. Ловцов Д.А., Кабелев Д.Б. Технология и проблемы рационального управления ключевой информацией в АСУ // Труды XXIX Всеросс. науч.-техн. конф. «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем» (24—25 июня 2010 г.) в 5-ми тт. Т. 4 / РАО. Серпухов : Серп. воен. ин-т, 2010. С. 144—148.
12. Сунаид Х.А.С., Яковлев А.В. Состояние и перспективы развития государственной информационно-телекоммуникационной системы Йемена // Труды Науч.-прак. конф. «Информационные системы и процессы» (15 июня 2018 г.). Тамбов : Межд. инф. Нобелевский центр, 2018. С. 76—89.
13. Шенец Н.Н. Об идеальных модулярных схемах разделения секрета в кольцах многочленов от нескольких переменных // Труды Междунар. конгресса по информатике: «Информационные системы и технологии» (31 октября 2011 г.) / БГУ. Т. 1. Минск : БГУ, 2011. С. 169—173.
14. Шнайер Б. Разделение секрета // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М. : Триумф, 2002. С. 93—96.
15. Шнайер Б. Алгоритмы разделения секрета // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М. : Триумф, 2002. С. 588—591.
16. Хучиров А.Г., Яковлев Ал.В., Яковлев Ан.В. Реализация метода кластерного анализа в математической модели процессов взаимообмена информационными ресурсами в АСУ специального назначения // Перспективы науки. № 1. Тамбов : Фонд развития науки и культуры, 2017. С. 75—79. ISSN 2077-6810.
17. Чмора А.Л. Современная прикладная криптография. 2-е изд., стер. М. : Гелиос АРВ, 2002. С. 123—124.

Рецензент: ***Алексеев Владимир Витальевич,*** *доктор технических наук, профессор, заведующий кафедрой информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов.*
E-mail: vvalex1961@mail.ru

SOFTWARE IMPLEMENTING THE SHAMIR ALGORITHM IN STRONG PRIVATE CRYPTOSYSTEMS

Viktor Gridnev, *Ph.D. (Technology), Associate Professor at the Information Systems and Information Protection Department of the Tambov State Technical University, Tambov, Russian Federation.*
E-mail: vikadres@yandex.ru

Aleksandr Selivanov, *5th year student at the Tambov State Technical University, Tambov, Russian Federation.*
E-mail: istrebion@yandex.ru

Keywords: *software, cryptosystem, encryption key, depositing, secret sharing threshold scheme, algorithm, shadow authentication control, security, information system, user.*

Abstract.

Purposes of the paper: facilitating the user's work in sharing a secret based on application software implementing a system for depositing encryption keys in strong private cryptosystems using the Shamir threshold scheme.

Methods used: object-oriented programming, simulation modelling.

Results obtained: a justification was given for the need to use strong private cryptosystems with key depositing. Topical cases of using such systems were presented. A software package for key depositing based on the Shamir threshold scheme was developed. Legal issues of depositing keys in private cryptosystems were studied.

The software package includes a programme providing a simple interface for separating and restoring secrets as well as a programme embedded in third-party software in the form of a header library. The main feature of the software package is simplicity, using it doesn't require special qualifications.

References

1. Alekseev V.V., Strel'tsov A.A., Emel'ianov E.V. Pravovoi podkhod k postroeniiu zashchity informatsii v organizatsii. Pravovaia informatika, 2020, No. 2, pp. 54-61. DOI: 10.21681/1994-1404-2020-2-54-61 .
2. Bolotov A.A., Gashkov S.B., Frolov A.B., Chasovskikh A.A. Elementarnoe vvedenie v ellipticheskuiu kriptografiiu. Algebraicheskie i algoritmicheskie osnovy. M. : KomKniga, 2006. 328 pp.
3. Buch G., Rambo Dzh., Dzhekobson A. Iazyk UML. Rukovodstvo pol'zovatelia. 2-e izd. SPb. : DMK Press, 2004. 432 pp.
4. Gridnev V.A., Volodin I.S., Zheludkova A.M. Organizatsionno-pravovye voprosy vnedreniia stoikikh chastnykh kriptosistem. Pravovaia informatika, 2021, No. 1, pp. 51-60. DOI: 10.21681/1994-1404-2021-1-51-60 .
5. Kernigan B.U., Ritchi D.M. Iazyk programmirovaniia C. M. : Vil'iams, 2009. 304 c.
6. Larman K. Primenenie UML 2.0 i shablonov proektirovaniia. 3-e izd. M. : Vil'iams, 2006. 736 pp.
7. Lovtsov D.A. Sistemologiia pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere : monografiia. M.: RGUP, 2016. 316 pp. ISBN 978-5-93916-505-1.
8. Lovtsov D.A. Informatsionno-pravovye osnovy pravoprimeneniia v tsifrovoi sfere. Monitoring pravoprimeneniia, 2020, No. 2(35), pp. 44-52. DOI: 10.21681/2226-0692-2020-2-44-52 .
9. Lovtsov D.A. Informatsionnaia bezopasnost' avtomatizirovannykh blokchein-sistem: ugrozy i sposoby povysheniia. Tr. II Mezhdunar. nauch.-prak. konf. "Transformatsiia natsional'noi sotsial'no-ekonomicheskoi sistemy Rossii" (22 noiabria 2019 g.), RGUP. M. : RGUP, 2020, pp. 464-473. ISBN 978-5-93916-823-6.
10. Lovtsov D.A. Problema garantirovannogo obespecheniia informatsionnoi bezopasnosti krupnomasshtabnykh avtomatizirovannykh sistem. Pravovaia informatika, 2017, No. 3, pp. 66-74. DOI: 10.21681/2226-0692-2017-3-66-74 .
11. Lovtsov D.A., Kabelev D.B. Tekhnologiia i problemy ratsional'nogo upravleniia kliuchevoi informatsiei v ASU. Trudy XXIX Vseross. nauch.-tekhn. konf. "Problemy effektivnosti i bezopasnosti funktsionirovaniia slozhnykh tekhnicheskikh i informatsionnykh sistem" (24-25 iiunia 2010 g.) v 5-mi tt., t. 4, RAO. Serpukhov : Serp. voen. in-t, 2010, pp. 144-148.
12. Sunaid Kh.A.S., Iakovlev A.V. Sostoianie i perspektivy razvitiia gosudarstvennoi informatsionno-telekommunikatsionnoi sistemy Iemena. Trudy Nauch.-prak. konf. "Informatsionnye sistemy i protsessy" (15 iiunia 2018 g.). Tambov : Mezhd. inf. Nobelevskii tsentr, 2018, pp. 76-89.
13. Shenets N.N. Ob ideal'nykh moduliarnykh skhemakh razdeleniia sekreta v kol'tsakh mnogochlenov ot neskol'kikh peremennykh. Trudy Mezhdunar. kongressa po informatike: "Informatsionnye sistemy i tekhnologii" (31 oktiabria 2011 g.), BGU, t. 1. Minsk : BGU, 2011, pp. 169-173.
14. Shnaier B. Razdelenie sekreta. Prikladnaia kriptografiia. Protokoly, algoritmy, iskhodnye teksty na iazyke Si. M. : Triumf, 2002, pp. 93-96.
15. Shnaier B. Algoritmy razdeleniia sekreta. Prikladnaia kriptografiia. Protokoly, algoritmy, iskhodnye teksty na iazyke Si. M. : Triumf, 2002, pp. 588-591.
16. Khuchirov A.G., Iakovlev Al.V., Iakovlev An.V. Realizatsiia metoda klasternogo analiza v matematicheskoi modeli protsessov vzaimoobmena informatsionnymi resursami v ASU spetsial'nogo naznacheniia. Perspektivy nauki, No. 1. Tambov : Fond razvitiia nauki i kul'tury, 2017, pp. 75-79. ISSN 2077-6810.
17. Chmora A.L. Sovremennaia prikladnaia kriptografiia. 2-e izd., ster. M. : Gelios ARV, 2002, pp. 123-124.

СПОСОБЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ АНОНИМНОСТИ В ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ

*Карпов Д.С., Ибрагимова З.А.**

***Ключевые слова**: анонимность, анонимизация, DarkNet, шифрование, метаданные, прокси-сервер, VPN, SSL-сертификат, TOR, интернет-сервис.*

Аннотация.

Цель исследования: анализ и обоснование причин, по которым пользователи стремятся обеспечить свою анонимность в Интернете, выявление субъектов, решающих задачи деанонимизации пользователей, определение наиболее эффективных способов и средств обеспечения анонимности в Интернете.

Методы и материалы. Использовались: результаты научных исследований в области анонимизации действий пользователей в Интернете, опубликованные в открытых источниках, включая результаты авторов; материалы, полученные авторами в ходе планирования, подготовки и проведения лабораторных и практических занятий со студентами, обучающимися по направлению подготовки «Информационная безопасность»; комплексный анализ и материалы исследований в данной предметной области.

Результаты: научное исследование и обоснование причин, по которым пользователи стремятся обеспечить свою анонимность в Интернете; определение субъектов, решающих задачи деанонимизации пользователей в Интернете; определение наиболее эффективных и часто используемых способов и средств обеспечения анонимности в Интернете.

Полученные результаты могут быть использованы для совершенствования научной и методической базы исследований в сфере информационной безопасности в областях, связанных с обеспечением анонимности и деанонимизации пользователей глобальной сети Интернет.

DOI: 10.21681/1994-1404-2021-3-60-67

Под *анонимностью* в сети Интернет можно понимать отсутствие личных данных о пользователях. На сегодняшний день существует множество причин, по которым пользователи хотят скрывать свои данные. Это стремление полностью защититься от возможных противоправных действий со стороны третьих лиц, осуществление противоправных действий в Интернете (например, *Internet scam*), доступ к *DarkNet* и др.

Есть и иные причины, по которым пользователи стремятся к своей анонимности, это, в частности:

Свобода выражения мнения. Многие боятся говорить то, что они действительно думают, поэтому прячутся за своим ником в социальной сети. Кто-то даже создает по несколько аккаунтов, что помогает им общаться так открыто, как они никогда не смогли бы в реальной жизни.

Конфиденциальность. Многие не хотят, чтобы другие что-то знали об их личной жизни, но рассказать о ней хочется. Поэтому они могут создавать аккаунты от другого имени и скрываться за ником.

Низкая самооценка. Многие в Интернете совсем не такие, какие в жизни. Они часто боятся показаться глупыми, нелепыми. Пытаются сохранить свою анонимность, ведь так они смогут обрести полную свободу, быть собой, не стесняться, что другие воспримут их странными.

Возможность решать «деликатные» вопросы анонимно. Есть еще одна важная категория людей, которые извлекают выгоду из анонимности — это те, кому нужно больше информации по какой-то теме, но они не хотят, чтобы их поймали на поиске этой информации.

Стеснение. Почти каждому человеку присуще стеснение. Кто-то просто не хочет, чтобы другие знали, что это именно он выставил какой-то текст или фотографию. Они не готовы рассказать всем о своих симпатиях, взглядах на жизнь, поэтому и пытаются спрятаться за всевозможными аккаунтами.

Злость. К сожалению, вымещение злости и ненависти на людей — одна из причин, по которой люди действуют анонимно. Такие люди хотят вылить грязь на других, не неся при этом за это ответственности. Они

* ***Карпов Дмитрий Сергеевич,*** *кандидат технических наук, доцент, доцент Российского экономического университета им. Г. В. Плеханова, г. Москва, Российская Федерация.*
E-mail: kds-zn@mail.ru

Ибрагимова Заира Анзоровна, *студент Российского экономического университета им. Г. В. Плеханова, г. Москва, Российская Федерация.*
E-mail: z.ibragimova.z02@mail.ru

запугивают других, выражают свою ненависть, хамят, сквернословят и делают это анонимно и безнаказанно.

Самовыражение. В Интернете легко «самовыражаться». Далеко не всем нужна слава и пиар, и многие пытаются сохранить анонимность из нежелания, чтобы все знали, что какое-то произведение создали именно они.

В глобальной сети за пользователями могут следить такие субъекты, как интернет-провайдеры, государственные органы, владельцы интернет-сервисов и даже иностранные специальные службы (например, проект *Prism*[1] АНБ США). Отслеживание интернет-провайдерами — это практика, с помощью которой интернет-провайдеры записывают информацию об онлайн-подключениях и действиях. Это означает, что все — от истории поиска до переписки по электронной почте — отслеживается и регистрируется интернет-провайдером. Он может видеть онлайн-поиски, незашифрованную переписку по электронной почте, данные социальных сетей; пароли и информацию, которую вводят на незашифрованных веб-сайтах; информацию о сайтах, на которые заходят пользователи; о файлах/торрентах, которые они скачивают; криптовалютные транзакции; географическое местоположение при использовании мобильных устройств.

Хотя провайдер не всегда отслеживает интернет-активность пользователя, у него в центре обработки данных есть сервер, куда «зеркалируется» определенный трафик — сервер системы оперативно-розыскных мероприятий (СОРМ)[2]. Владельцы сервисов также следят за пользователями. Необходимо быть осторожным при использовании *Google Mail* в качестве рабочей/личной почты или браузера *Chrome*. Ведь в этом случае *Google* будет очень удобно и легко собирать информацию. Это касается и российских сервисов, например, ЯндексКрипта[3], *VK* и др.

Для обеспечения анонимности пользователю нужно стараться не использовать реальные имена/фамилии/даты рождения. В разных сервисах нужно использовать разные пароли. Иначе если взломают одно — взломают все. Пользователь должен заводить несколько аккаунтов с разными никами и разным типом активности. При получении письма от сайта с паролем в открытом виде важно понимать, что это ненадежный сайт, поскольку он хранит пароль пользователя в незашифрованном виде. Так пароль может быть продан либо украден. Нельзя забывать переходить в режим инкогнито[4] при регистрации, входе на важные сайты, а при необходимости передачи секретных данных по открытому каналу связи выполнять предварительное шифрование с помощью *PGP*. Пользователь также может разбить информацию на части и передать их по разным каналам. Например, пароль сказать при встрече, логин в *Telegram*, адрес отправить в *Instagram*. Регистрация и совершение входа в сервис пользователем должны происходить только в случае, если есть *https*. При регистрации или входе обязательно использование *VPN* (*virtual private network*). Так пользователь не засветит свой *IP*-адрес. Перед тем как выложить очередное фото в Интернет, важно проверить, не осталось ли там деанонимизирующих метаданных.

Метаданные фотографий — это информация, которая часто бывает полезной, однако опасной для тех, кто хочет обеспечить максимальную анонимность. Так называемые данные *EXIF* доступны для каждой фотографии независимо от того, с какого устройства она была сделана. Они рассказывают, как было создано изображение, где и когда. Они могут рассказать о параметрах камеры/смартфона. Они также показывают, как изображение было отредактировано в редакторе. Информацию о владельце кадра и не только может узнать любой желающий, потратив на это всего несколько минут.

По данным лаборатории Касперского[5] *Facebook*, *eBay*, *Instagram*, *Twitter*, *Craigslist*, *ВКонтакте* метаданные из фотографий удаляют; *Flickr, Google Photo, Google+, Tumblr,* ЦИАН — не удаляют.

Чтобы не распространить личную информацию вместе с фотографией, пользователю необходимо отключить функцию геолокации для камеры, а прежде чем разместить свою фотографию в Интернете, удалить метаданные. Для этого можно использовать *XnView*, потому что встроенный механизм *Windows* «Удаление свойств и личной информации» оставляет под контролем как миниатюру, так и блоки *EXIF*. Необходимо также запретить сохранение метаданных в настройках конфиденциальности сервисов. Однако если пользователю действительно есть что терять, лучше не публиковать то, что может сыграть против него в будущем.

Говоря об анонимности в Интернете, не стоит забывать о правильной настройке браузера. Есть несколько простых правил. *Во-первых*, нельзя сохранять свои пароли в браузере, необходимо заходить и регистрироваться в различных сервисах только через режим инкогнито. *Во-вторых*, браузер не должен устанавливать связь между пользовательскими файлами *cookie*/паролями/историей браузера и любой другой инфор-

[1] Проект *PRISM*. URL: https://www.securitylab.ru/news/tags/PRISM (дата обращения: 29.07.2021).

[2] Приказ Минкомсвязи России от 16 апреля 2014 г. № 83 (ред. от 15.04.2019) «Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть III. Правила применения оборудования коммутации и маршрутизации пакетов информации сетей передачи данных, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий» // Демоверсия СПС «КонсультантПлюс» (дата обращения: 29.05.2021).

[3] Ресурс ЯндексКрипта основан на методе машинного обучения и анализирует характерное поведение пользователей в Интернете. Для удачного исследования достаточно проанализировать поведение не менее 30 000 пользователей.

[4] Режим «инкогнито» в браузерах — это специальный режим, при котором не сохраняется история просмотров, загрузок и др.

[5] Эксперимент: проверяем, что интересного можно узнать из метаданных фотографий в Интернете. URL: https://www.kaspersky.ru/blog/exif-privacy/13506 (дата обращения: 29.05.2021).

мацией с неизвестными серверами в сети. *В-третьих*, браузер не должен сохранять *cookie* при перезапусках.

Для безопасной передачи файла пользователю необходимо использовать шифрование, например, *GPG* или *PGP*. *PGP* (*Pretty Good Privacy*) — система шифрования, используемая как для отправки зашифрованных писем, так и для шифрования конфиденциальных файлов. При отправке письма или файла, которые были зашифрованы и подписаны с помощью *PGP*, пользователь может быть уверен, что письмо не поддельное, и только получатель, указанный отправителем, сможет его прочитать. Таким образом, даже если почта будет взломана, злоумышленник не сможет получить доступ к электронным письмам и файлам.

Для шифрования любого файла с помощью *GPG* пользователю необходимо использовать команду «*gpg-c file*». Система дважды запросит пароль, и после шифрования рядом с пользовательским исходным файлом появится новый с расширением *.gpg*, например, 1.*gpg*. Для того чтобы расшифровать отправленный файл, необходимо воспользоваться командой «*gpg file*», потом ввести пароль и получить исходный файл. Однако у *gpg* шифрования есть свой недостаток: помимо передаваемых файлов и писем нужно передавать пароль. Поэтому гарантий того, что его не перехватит злоумышленник, нет. Эту проблему решает *асимметричная криптография* [11]. Она использует частные и открытые ключи для шифрования/дешифрования данных. Открытый ключ — один из ключей в паре, который может быть общим для всех, тогда как закрытый ключ — ключ в паре, который хранится в секрете. Хотя *открытый* ключ доступен каждому, *закрытый* ключ, необходимый для расшифровки данных, сохраняется у владельца.

Но что бы ни делал пользователь, если он все еще использует календарь *Google*, сохраняет свою переписку в почте Яндекса или хранит файлы в *Dropbox*, он не добьется своей анонимности. Чтобы интернет-серверы не могли следить за пользователем, необходимо навсегда ограничить их использование. Заменой *Dropbox* можно считать довольно много приложений с открытым исходным кодом (*open source*): *Seafile*, *OwnCloud*, *Sparkleshare*, *Pydio*.

Также важно построить защищенную операционную систему (ОС) на компьютере. Для этого необходимо перейти на *Linux* или другую ОС с открытым исходным кодом[6], использовать шифрование дисковых разделов и всегда создавать криптостойкий пароль (будет еще лучше, если аутентификация будет проходить по отпечатку пальца [14]).

Если пользователь хочет обеспечить свою анонимность при использовании телефона, ему необходимо: заменить стандартную прошивку *Android* на *Replicant/Cyanogenmod/Paranoid Android*, всегда использовать шифрование файловой системы и *VPN* для доступа в Интернет, переключиться с *Google Play* на *F-Droid*. Также необходимо использовать «длинный» криптографический пароль и следить за активностью телефона (при помощи приложения-трекера для слежения за своим телефоном онлайн, например, *Self-Hosted GPS Tracker* для Андроид).

В обеспечении анонимности может помочь сервер синхронизации *Firefox*. Например, когда у пользователя есть файл, который находится в двух или более местах, и он хочет, чтобы файл был одинаковым везде и всегда, необходимо синхронизировать его. Это происходит с помощью механизма *синхронизации*. Когда что-то изменяется в этом файле, механизм синхронизации будет реплицировать изменения во всех местах, где есть файл.

Учетная запись *Firefox* позволяет синхронизировать данные, такие как закладки, история, пароли, открытые вкладки и установленные дополнения на всех устройствах. Можно отключить синхронизацию в любое время, также как и изменить список данных, которые пользователь хочет синхронизировать. Однако нельзя включать синхронизацию на чужих, а тем более общедоступных устройствах, необходимо использовать на них режим инкогнито.

Создание корневого *SSL*[7]-сертификата позволит веб-сайтам переходить с *HTTP* на *HTTPS*, что более безопасно. *SSL*-сертификат — это файл данных, размещенный на исходном сервере веб-сайта. *SSL*-сертификаты делают возможным шифрование *SSL/TLS* и содержат открытый ключ и удостоверение веб-сайта. Устройства, пытающиеся связаться с исходным сервером, будут ссылаться на этот файл, чтобы получить открытый ключ и проверить личность сервера. Закрытый ключ хранится в секрете и защищен.

Проведенный анализ опубликованных научных работ [3—10, 15, 20, 21] в области анонимизации пользователей глобальной сети Интернет показал, что наиболее эффективными и часто используемыми в настоящее время являются такие способы обеспечения анонимности, как использование технологий *проксификации*, *VPN*, *Tor* и *I2P*, опирающихся на соответствующие программно-аппаратные средства. Рассмотрим их подробнее.

Если пользователь использует прокси-сервер [15], трафик проходит через него по пути к запрошенному адресу. Затем запрос возвращается через тот же прокси-сервер, а после прокси-сервер отправляет данные, полученные с веб-сайта. Возможно использование цепочек (каскадов) прокси-серверов (рис. 1).

[6] Анонимизация в Интернете и использование *self-hosted* сервисов. URL: https://habr.com/ru/post/237335 (дата обращения: 29.05.2021).

[7] *SSL* (*secure sockets layer* — уровень защищенных сокетов) — криптографический протокол для безопасной связи. С версии 3.0 *SSL* заменен на *TLS* (*transport layer security* — безопасность транспортного уровня), но название предыдущей версии прижилось, поэтому сегодня под *SSL* чаще всего подразумевают *TLS*. Любой веб-сайт с *https*-адресом использует *SSL/TLS*.

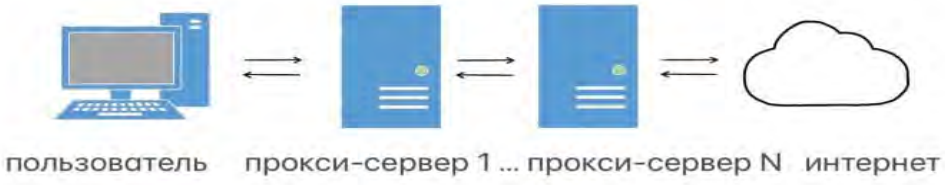

Рис. 1. Использование каскада прокси-серверов для анонимизации

Рис. 2. Использование технологии VPN для анонимизации

По обеспечению анонимности прокси-серверы можно разделить на *HTTP*-(веб)-прокси-серверы, *HTTPS*-(веб)-прокси-серверы, *SOCKS*[8]-прокси-серверы, *CGI*-прокси.

HTTP-(веб)-прокси-серверы — наиболее распространенный тип прокси, предназначенный в первую очередь для посещения веб-сайтов, загрузки и передачи файлов. Как следует из названия, прокси работают по протоколу *HTTP*, что позволяет быстро и эффективно работать с веб-страницами. *HTTPS*-прокси являются модификацией *HTTP*-прокси. Буква «*s*» в конце означает «безопасный». Такие прокси поддерживают шифрование данных для повышения безопасности данных в Интернете. Это достигается с помощью криптографических протоколов *SSL* и *TLS*. У *SOCKS*-прокси-серверов самый универсальный протокол, когда дело доходит до прокси-серверов. Эти прокси не передают никаких *HTTP*-заголовков, что делает их анонимными по умолчанию, скрывая реальный *IP*-адрес клиента и факт использования прокси. *CGI*-прокси — это веб-страница, которая схожа со страницами поисковых систем. Но вместо поисковых фраз в поле ввода пользователь вписывает *URL* того сайта, на который хочет перейти. После нажатия кнопки *Submit/Go* он автоматически попадает на страницу, *URL* которой указал.

Преимуществом прокси-серверов является то, что они очень дешевы, а иногда и вовсе бесплатны. Однако есть и свои *недостатки*: прокси-серверы используют данные кэша и могут запоминать всю личную информацию, включая пароли. Кроме того, нужно настраивать прокси-сервер под каждое приложение.

Технология *VPN* — это технология, которая создает логическую сеть поверх другой сети [2, 16—19]. *VPN* создает зашифрованный туннель между пользователем и удаленным сервером. Весь интернет-трафик направляется через этот туннель, так что пользовательские данные защищены от посторонних глаз на этом пути. Поскольку трафик выходит из *VPN*-сервера, истинный *IP*-адрес скрыт, маскируя личность и местоположение (рис. 2). В зависимости от применяемых протоколов и назначения, *VPN* поддерживает соединения трех видов: «клиент-клиент», «клиент-сеть» и «сеть-сеть». Говоря о *VPN*, не стоит забывать о *SSH*[9]-туннелях. Хотя между ними и есть различия, принцип работы у них очень схож.

Сейчас провайдерами предлагаются *PPTP*, *L2TP/IPSec*, *OpenVPN* и *SSTP* протоколы *VPN*. *PPTP* является наиболее широко используемым, быстрым, простым в настройке, однако устаревшим, отчего защита данных подвергается серьезному риску. У протокола *L2TP/IPSec* *L2TP* отвечает за транспорт, а *IPSec* за шифрование [13]. Используемые вместе *L2TP* и *IPSec* гораздо более безопасны, чем *PPTP*, но все же больше подходят для анонимизации [1], чем для обеспечения безопасности [12]. *OpenVPN* — это относительно новый и легко настраиваемый протокол. Самое лучшее в *OpenVPN* то, что он имеет открытый исходный код. В сочетании с сильным алгоритмом шифрования он является одним из самых безопасных доступных протоколов *VPN*, однако требует отдельного программного клиента. *SSTP* — это

[8] *SOCKS* (сокращение от «*SOCKet Secure*») — интернет-протокол, который используется для передачи пакетов с данными от сервера к клиенту с помощью промежуточного прокси-сервера. На сегодня это наиболее продвинутая массовая технология для организации прокси.

[9] *SSH* — сетевой протокол прикладного уровня, предназначенный для «туннелирования» сетевого трафика с использованием зашифрованного соединения.

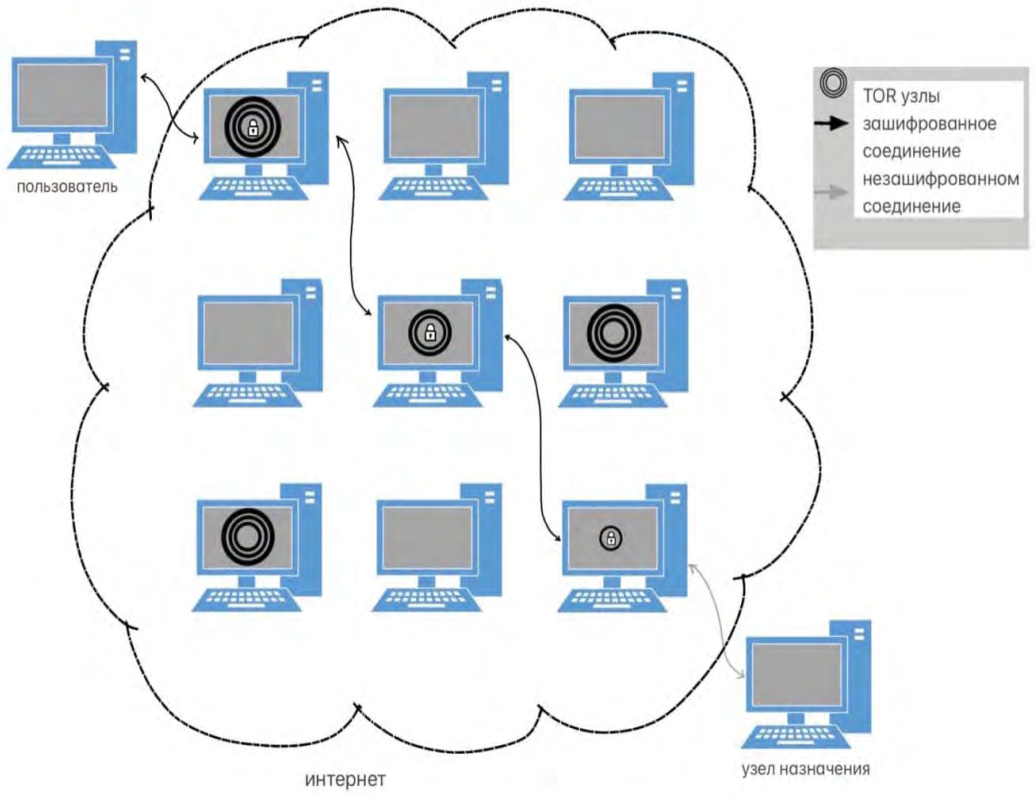

Рис. 3. Использование технологии TOR для анонимизации

VPN-протокол, который разработан *Microsoft*. Протокол предназначен для защиты данных и трафика и считается более безопасным, чем *PPTP* или *L2TP/IPSec*.

К преимуществам *VPN/SSH* относится то, что использовать их быстро и удобно, а также не требуется отдельная настройка приложений. Однако, как и в случае с прокси-серверами, нужно доверять *VPN/SSH*-серверу/провайдеру.

Когда пользователь подключается к *TOR*, его *исходящий* интернет-трафик перенаправляется через случайную серию, состоящую по крайней мере из трех узлов (ретрансляторов), прежде чем достичь места назначения (веб-сайта, который пользователь хочет посетить) [3, 5, 10]. Компьютер подключен к узлу входа; конечным узлом, через который проходит трафик, является узел выхода, после чего он достигает места назначения. *Входящий* трафик перенаправляется аналогичным образом. Помимо прохождения через несколько узлов, трафик многократно шифруется. Он теряет уровень шифрования на каждом узле, но никогда полностью не расшифровывается, пока не покинет выходной узел для назначения (рис. 3). *TOR* решает главную задачу: довольно-таки высокий уровень анонимности пользователя при передаче только *http*-трафика. Однако, как и все другие реально существующие анонимизирующие сети с малыми задержками, *TOR* не может защитить от глобального наблюдателя [4].

Преимущества *TOR* — обеспечение высокого уровня безопасности пользователя; любой пользователь может легко воспользоваться *TOR* , для этого достаточно скачать *TOR Browser Bundle*. Недостатки *TOR* — прослушивание выходного трафика, низкая скорость работы и наличие управляющих серверов.

I2P — это децентрализованная анонимизирующая сеть, построенная с использованием *Java* на тех же принципах, что и *TOR*, но изначально задуманная как автономный *DarkNet*.

В *I2P* есть два главных понятия:

- «туннель» — временный однонаправленный путь через некоторый список узлов;
- «сетевая база *NetDb*» — документирование группы точек входа в туннель (*leases*) для конкретного клиентского назначения, которая хранит в себе *RouterInfos* — контактная информация маршрутизатора (клиентов) и *LeaseSets* — контактная информация назначения.

Таким образом, определены причины, по которым пользователи стремятся обеспечить свою анонимность в сети Интернет, субъекты, решающие задачи деанонимизации пользователей в Интернете, наиболее эффективные и часто используемые способы и средства обеспечения анонимности в Интернете. Важно заметить, что ни один из приведенных способов не гарантирует полной анонимности, но их вполне достаточно, чтобы значительно усложнить задачу деанонимизации.

Полученные результаты можно использовать для совершенствования научной и методической базы исследований в сфере информационной безопасности в областях, связанных с обеспечением анонимности и деанонимизации пользователей глобальной сети Интернет.

Литература

1. Борисов Р.С., Ефименко А.А. Регламент обработки наборов данных для их публикации в открытых источниках // Правовая информатика. 2021. № 2. С. 59—70. DOI: 10.21681/1994-1404-2021-2-59-70 .
2. Карпов Д.С., Микрюков А.А., Козырев П.А. Повышение качества подготовки специалистов по направлению подготовки «Информационная безопасность» // Открытое образование. 2019. Т. 23. № 6. С. 22—29. DOI: 10.21686/1818-4243-2019-6-22-29 .
3. Карпов Д.С., Спивак А.И. Об одном способе воздействия на информационные ресурсы, имеющие выход в сеть Интернет // Труды Междунар. науч.-прак. конф. «Ценности и интересы современного общества». Часть 3: «Современные парадигмы информационных технологий в развитии общества» / МЭСИ. М. : МЭСИ, 2015. С. 88—93.
4. Карпов Д.С., Спивак А.И. Разработка модели угроз безопасности информации в системе информационного обмена на основе технологии анонимизации TOR // Труды XXXVII Всеросс. науч.-техн. конф. «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем» / Филиал ВА РВСН. Серпухов : ФВА РВСН им. Петра Великого, 2018. С. 97—101.
5. Карпов Д.С., Спивак А.И. Использование технологий анонимизации трафика для воздействия на информационные ресурсы // Труды Междунар. науч.-прак. конф. «Актуальные задачи математического моделирования и информационных технологий» / Сочинский ГУ. Сочи : Соч. гос. ун-т, 2015. С. 93—97.
6. Карпов Д.С., Спивак А.И. Создание математической модели обеспечения достаточного уровня анонимности в системах передачи данных с сохранением целостности и конфиденциальности передаваемой информации // Проблемы обеспечения информационной безопасности в ВС РФ : сб. науч. тр. № 1. Краснодар : КВВУ, 2016. С. 133—143.
7. Карпов Д.С., Спивак А.И. Обеспечение достаточного уровня анонимности отправителя в распределенной компьютерной системе информационного обмена // «Известия» № 265 : науч.-техн. сб. Часть I «Перспективные АСУ и робототехнические комплексы военного назначения». Балашиха : ВА РВСН, 2016. С. 155—164.
8. Карпов Д.С., Спивак А.И. Разработка алгоритма анонимного обмена информацией в системах передачи данных с сохранением ее целостности и конфиденциальности // Проблемы обеспечения информационной безопасности в ВС РФ : сб. науч. тр. № 1. Краснодар : КВВУ, 2016. С. 112—121.
9. Карпов Д.С., Спивак А.И. Реализация способа обеспечения анонимности отправителя в информационно-телекоммуникационной сети международного информационного обмена // Труды Междунар. науч.-прак. конф. «Информационная безопасность: вчера, сегодня, завтра» / РГГУ. М. : РГГУ, 2018. С. 127—135.
10. Киселенко В.А. Анонимизация работы в глобальной компьютерной сети Internet // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение». 2005. № 1. С. 43—51.
11. Ловцов Д.А. Теория защищенности информации в эргасистемах : монография. М. : Рос. гос. ун-т правосудия, 2021. 276 с. ISBN 978-5-93916-896-0.
12. Ловцов Д.А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. 2017. № 3. С. 66—74.
13. Ловцов Д.А. Обеспечение информационной безопасности в российских телематических сетях // Информационное право. 2012. № 4. С. 3—7.
14. Ловцов Д.А., Князев К.В. Защищённая биометрическая идентификация в системах контроля доступа. I. Математические модели и алгоритмы // Информация и космос. 2013. № 1. С. 100—103.
15. Маркин Д.О., Архипов П.А., Галкин А.С. Исследование устойчивости анонимной сети на основе технологий веб-прокси // Вопросы кибербезопасности. 2016. № 2 (15). С. 21—27.
16. Наполова Е.И., Кожевников С.В. Защита компьютерных сетей на основе технологии virtual private network // Экономика и качество систем связи. 2018. № 2. С. 80—85.
17. Росляков А. Виртуальные частные сети VPN. Модели и методы анализа. LAP, 2011. 328 с.
18. Росляков А.В. Виртуальные частные сети: основы построения и применения : монография. М. : Эко-Трендз, 2006. 300 с.
19. Рябко Е.И. Калейдоскоп VPN-технологий // T-Comm. 2009. Спецвып. по ИБ. С. 16—20.
20. Сергеев С.М. Некоторые проблемы противодействия использованию в преступной деятельности средств обеспечения анонимизации пользователя в сети Интернет // Вестник СПб. ун-та МВД России. 2017. № 1 (73). С. 137—140.
21. Karpov D.S., Spivak A.I. The use of technology for traffic anonymization exposure to information resources // European Journal of Computer Science. 2015. № 1 (1). Pp. 34-40.

Рецензент: ***Марков Алексей Сергеевич,*** *доктор технических наук, старший научный сотрудник, генеральный директор НПО «Эшелон», профессор кафедры информационной безопасности МГТУ им. Э. Н. Баумана, г. Москва. E-mail: a.markov@bmstu.ru*

WAYS AND MEANS TO ENSURE ANONYMITY IN THE GLOBAL INTERNET NETWORK

Dmitrii Karpov, *Ph.D. (Technology), Associate Professor at the Plekhanov Russian University of Economics, Moscow, Russian Federation.*
E-mail: kds-zn@mail.ru

Zaira Ibragimova, *student at the Plekhanov Russian University of Economics, Moscow, Russian Federation.*
E-mail: z.ibragimova.z02@mail.ru

Keywords: *anonymity, anonymisation, DarkNet, encryption, metadata, proxy server, VPN, SSL certificate, TOR, Internet service.*

Abstract.

Purpose of the study: analysing and justificating the reasons why users seek to ensure their anonymity on the Internet, identifying subjects solving the tasks of deanonymising users, finding the most efficient ways and means of ensuring anonymity on the Internet.

Methods and materials used: results of research in the field of anonymisation of user actions on the Internet published in open sources, including the results obtained by the authors, materials obtained by the authors in the course of planning, preparing and carrying out laboratory and practical training of students studying in the subject of information security, multi-faceted analysis and materials of research in this subject area.

Results obtained: a research study and justification of reasons why users seek to ensure their anonymity on the Internet, identification of subjects solving the tasks of deanonymising users on the Internet, finding the most efficient and frequently used ways and means of anonymisation on the Internet.

The obtained results can be used to improve the research and methodological basis for research in the field of information security in areas related to anonymisation and deanonymisation of users in the global Internet network.

References

1. Borisov R.S., Efimenko A.A. Reglament obrabotki naborov dannykh dlia ikh publikatsii v otkrytykh istochnikakh. Pravovaia informatika, 2021, No. 2, pp. 59-70. DOI: 10.21681/1994-1404-2021-2-59-70 .
2. Karpov D.S., Mikriukov A.A., Kozyrev P.A. Povyshenie kachestva podgotovki spetsialistov po napravleniiu podgotovki "Informatsionnaia bezopasnost'". Otkrytoe obrazovanie, 2019, t. 23, No. 6, pp. 22-29. DOI: 10.21686/1818-4243-2019-6-22-29 .
3. Karpov D.S., Spivak A.I. Ob odnom sposobe vozdeistviia na informatsionnye resursy, imeiushchie vykhod v set' Internet. Trudy Mezhdunar. nauch.-prak. konf. "Tsennosti i interesy sovremennogo obshchestva". Chast' 3: "Sovremennye paradigmy informatsionnykh tekhnologii v razvitii obshchestva", MESI. M. : MESI, 2015, pp. 88-93.
4. Karpov D.S., Spivak A.I. Razrabotka modeli ugroz bezopasnosti informatsii v sisteme informatsionnogo obmena na osnove tekhnologii anonimizatsii TOR. Trudy XXXVII Vseross. nauch.-tekhn. konf. "Problemy effektivnosti i bezopasnosti funktsionirovaniia slozhnykh tekhnicheskikh i informatsionnykh sistem", filial VA RVSN. Serpukhov : FVA RVSN im. Petra Velikogo, 2018, pp. 97-101.
5. Karpov D.S., Spivak A.I. Ispol'zovanie tekhnologii anonimizatsii trafika dlia vozdeistviia na informatsionnye resursy. Trudy Mezhdunar. nauch.-prak. konf. "Aktual'nye zadachi matematicheskogo modelirovaniia i informatsionnykh tekhnologii", Sochinskii GU. Sochi : Soch. gos. un-t, 2015, pp. 93-97.
6. Karpov D.S., Spivak A.I. Sozdanie matematicheskoi modeli obespecheniia dostatochnogo urovnia anonimnosti v sistemakh peredachi dannykh s sokhraneniem tselostnosti i konfidentsial'nosti peredavaemoi informatsii. Problemy obespecheniia informatsionnoi bezopasnosti v VS RF : sb. nauch. tr. No. 1. Krasnodar : KVVU, 2016, pp. 133-143.
7. Karpov D.S., Spivak A.I. Obespechenie dostatochnogo urovnia anonimnosti otpravitelia v raspredelennoi komp'iuternoi sisteme informatsionnogo obmena. "Izvestiia" No. 265 : nauch.-tekhn. sb. Chast' I "Perspektivnye ASU i robototekhnicheskie kompleksy voennogo naznacheniia". Balashikha : VA RVSN, 2016, pp. 155-164.
8. Karpov D.S., Spivak A.I. Razrabotka algoritma anonimnogo obmena informatsiei v sistemakh peredachi dannykh s sokhraneniem ee tselostnosti i konfidentsial'nosti. Problemy obespecheniia informatsionnoi bezopasnosti v VS RF : sb. nauch. tr. No. 1. Krasnodar : KVVU, 2016, pp. 112-121.
9. Karpov D.S., Spivak A.I. Realizatsiia sposoba obespecheniia anonimnosti otpravitelia v informatsionno-telekommunikatsionnoi seti mezhdunarodnogo informatsionnogo obmena. Trudy Mezhdunar. nauch.-prak. konf. "Informatsionnaia bezopasnost': vchera, segodnia, zavtra", RGGU. M. : RGGU, 2018, pp. 127-135.

10. Kiselenko V.A. Anonimizatsiia raboty v global'noi komp'iuternoi seti Internet. Vestnik MGTU im. N.E. Baumana, ser. "Priborostroenie", 2005, No. 1, pp. 43-51.
11. Lovtsov D.A. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : Ros. gos. un-t pravosudiia, 2021. 276 s. ISBN 978-5-93916-896-0.
12. Lovtsov D.A. Problema garantirovannogo obespecheniia informatsionnoi bezopasnosti krupnomasshtabnykh avtomatizirovannykh sistem. Pravovaia informatika, 2017, No. 3, pp. 66-74.
13. Lovtsov D.A. Obespechenie informatsionnoi bezopasnosti v rossiiskikh telematicheskikh setiakh. Informatsionnoe pravo, 2012, No. 4, pp. 3-7.
14. Lovtsov D.A., Kniazev K.V. Zashchishchennaia biometricheskaia identifikatsiia v sistemakh kontrolia dostupa. I. Matematicheskie modeli i algoritmy. Informatsiia i kosmos, 2013, No. 1, pp. 100-103.
15. Markin D.O., Arkhipov P.A., Galkin A.S. Issledovanie ustoichivosti anonimnoi seti na osnove tekhnologii veb-proksi. Voprosy kiberbezopasnosti, 2016, No. 2 (15), pp. 21-27.
16. Napolova E.I., Kozhevnikov S.V. Zashchita komp'iuternykh setei na osnove tekhnologii virtual private network. Ekonomika i kachestvo sistem sviazi, 2018, No. 2, pp. 80-85.
17. Rosliakov A. Virtual'nye chastnye seti VPN. Modeli i metody analiza. LAP, 2011. 328 s.
18. Rosliakov A.V. Virtual'nye chastnye seti: osnovy postroeniia i primeneniia : monografiia. M. : Eko-Trendz, 2006. 300 s.
19. Riabko E.I. Kaleidoskop VPN-tekhnologii. T-Comm, 2009, spetsvyp. po IB, pp. 16-20.
20. Sergeev S.M. Nekotorye problemy protivodeistviia ispol'zovaniiu v prestupnoi deiatel'nosti sredstv obespecheniia anonimizatsii pol'zovatelia v seti Internet. Vestnik SPb. un-ta MVD Rossii, 2017, No. 1 (73), pp. 137-140.
21. Karpov D.S., Spivak A.I. The use of technology for traffic anonymization exposure to information resources. European Journal of Computer Science, 2015, No. 1 (1), pp. 34-40.

МОДЕЛИРОВАНИЕ АДАПТАЦИИ ЭЛЕКТРОННЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ ДЛЯ СЛАБОВИДЯЩИХ И НЕЗРЯЧИХ ПОЛЬЗОВАТЕЛЕЙ

*Алексеев В.В., Дубровина О.В.**

***Ключевые слова**: электронные информационные ресурсы, невизуальный доступ, брайлевский дисплей, принтер Брайля, программа экранного доступа, синтезаторы речи, тифлоинформационные средства и технологии.*

Аннотация.

Цель работы: выявить и определить пути разрешения проблем, ограничивающих возможности слабовидящих и незрячих пользователей по доступу к электронным информационным ресурсам.

Методы: информационно-правовой анализ, концептуально-логическое моделирование, количественный анализ, метод самоотбора.

Результаты: выявлены основные проблемы доступа слабовидящих и незрячих пользователей к электронным информационным ресурсам; исследованы механизмы и необходимые средства доступа к электронным информационным ресурсам; разработаны модели работы и адаптации электронных информационных ресурсов к потребностям незрячего пользователя; определены пути решения проблемных моментов доступа слабовидящих и незрячих пользователей к электронным информационным ресурсам.

DOI: 10.21681/1994-1404-2021-3-68-76

Введение

Стандартный интерфейс компьютера ориентирован на зрячих людей и основан на визуально воспринимаемых формах представления информации. Возможность работать на компьютере для незрячих обеспечивается за счет комплекса специальных программных и аппаратных — тифлоинформационных (от греч. *τυφλός (typhlós)*, «слепой») — средств, преобразующих визуальную информацию в осязательную и слуховую[1] [1, 5, 7, 10, 12, 14].

Доступ слабовидящих и незрячих пользователей к электронным информационным ресурсам

Важнейшим источником отличий между процессами работы на основе стандартного (визуального) и невизуального интерфейса становится принципиальное различие *информационных моделей* [8], на основе которых они строятся. В стандартном варианте целостное представление о рабочей ситуации может дать изображение на экране. При работе же незрячего пользователя информационная модель рабочей ситуации строится на основе сообщений программы экранного доступа. Эта модель не имеет материального носителя, существуя только в представлении пользователя.

На основе анализа основных аспектов работы незрячего пользователя за персональным компьютером можно определить структурную модель его работы с учетом тифлоинформационных средств (рис. 1).

То есть для работы за компьютером незрячему пользователю необходимы тифлоинформационные средства, позволяющие взаимодействовать с системой без помощи посторонних.

Основными известными тифлоинформационными средствами (тифлосредствами) в настоящее время являются [5, 10, 12]: программы экранного доступа; синтезаторы речи; брайлевские дисплеи; принтеры Брайля.

Главным компьютерным тифлосредством является программа экранного доступа, осуществляющая передачу информации между незрячим пользователем и компьютером. Это происходит благодаря выводу информации при помощи звука и рельефно-точечного вывода. Программа считывает текст на мониторе, выводя его в удобном для пользователя виде.

[1] Земцова М. И. Методы и тифлотехнические средства обучения в школе слепых. М. : Просвещение, 1964. 72 с.

* ***Алексеев Владимир Витальевич,*** *доктор технических наук, профессор, заведующий кафедрой информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*
E-mail: vvalex1961@yandex.ru

Дубровина Оксана Васильевна, *аспирант кафедры информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*
E-mail: prepov@rambler.ru

Рис. 1. Структурная модель работы незрячего пользователя

Наибольшей популярностью пользуются программы экранного доступа для персонального компьютера: *JAWS*, разработанная группой незрячих и слабовидящих людей из компании *Freedom Scientific* в США (г. Сент-Питерсберг, штат Флорида), и *NVDA*, разработанная незрячими программистами Майклом Керраном и Джеймсом Техом (Австралия). Для смартфонов применяются в основном программа экранного доступа *VoiceOver*, если это смартфон с операционной системой *Mac OS X*, и *TalkBack* для устройств на базе операционной системы *Android* [4, 10, 11, 14].

Аппаратные и программные *синтезаторы речи* осуществляют голосовой вывод информации. Они представляют собой программы, преобразующие в устную речь цифровую информацию, которую считывают программы экранного доступа. По мнению большинства слабовидящих и незрячих пользователей, важными параметрами синтезаторов речи являются: качество речи, быстрота реакции на управляющее воздействие и максимально возможная скорость воспроизведения.

Для вывода рельефно-точечного вида компьютерной информации используют специальное устройство, называемое *брайлевским дисплеем*. Работа незрячего с брайлевским дисплеем представляет собой просмотр содержимого монитора через небольшое окно, на котором отображается вся информация, расположенная на экране. Но перемещение окна брайлевского дисплея ограничивается программой экранного доступа, так как нет возможности прочитать одновременно всю информацию на экране компьютера.

Большинство брайлевских дисплеев могут не только выводить информацию, но и передавать компьютеру управляющее воздействие пользователя. Каждый модуль дисплея снабжен специальной кнопкой, нажатие на которую передает компьютеру информацию об отображаемой этим модулем позиции на экране и может интерпретироваться программным обеспечением (например, как нажатие кнопки «мыши», вызывая перемещение каретки или активизацию соответствующего пункта меню).

При работе за компьютером незрячий пользователь применяет обычную клавиатуру. Вся работа строится на знании десятипальцевого метода печати и набора команд управления ОС *Windows* [5, 10, 11].

Существует также *брайлевская клавиатура*. Это устройство, которое позволяет вводить текстовые символы в 6- или 8-точечном брайлевском представлении. Каждая брайлевская клавиатура имеет по крайней мере 6 клавиш для ввода точек, клавишу для ввода пробела и, в зависимости от модели, дополнительные служебные клавиши.

Для вывода информации на печать применяются специальные принтеры, они позволяют преобразовывать плоскопечатный текст в шрифт Брайля. Современные *брайлевские принтеры* позволяют выводить на печать тексты, выполненные в любом текстовом редакторе. Графический вывод на брайлевский принтер используется чаще всего для печати планов, схем, графиков и др. Разумеется, изобразительные возможности и разрешающая способность рельефно-точечной графики существенно уступают обычным.

Для полноценного доступа к необходимой информации слабовидящих и незрячих пользователей все ресурсы и документы в сети Интернет должны быть адаптированы к их потребностям. С позиции *теории систем* [9] рассматриваемые информационные ресурсы, а также средства хранения, обработки и представления информации образуют целенаправленную систему, для которой действия слабовидящих и незрячих пользователей являются возмущающим воздействием. На основе этого построена *модель адаптации электронных информационных ресурсов* (ЭИР) для слабовидящих и незрячих пользователей (рис. 2).

Модель отражает общий принцип работы слабовидящих и незрячих пользователей с ЭИР, определяет место тифлоинформационных технологий в работе пользователя, показывает основные взаимосвязи.

Рис. 2. Модель адаптации электронных информационных ресурсов для слабовидящих и незрячих пользователей

Правовые аспекты адаптации информационных ресурсов

В настоящее время тифлоинформационные средства не решают всех проблем ограничения доступа к электронным информационным ресурсам. Наряду с их применением необходимо также соблюдение существующих стандартов в сфере разработки информационных ресурсов. В частности, важнейшим аспектом применения электронных информационных ресурсов является возможность получения образования. Согласно Федеральному закону от 29 декабря 2012 г. № 273-ФЗ (ред. от 30.04.2021) «Об образовании в Российской Федерации» (ст. 79), *«организация получения образования обучающимися с ограниченными возможностями здоровья, все учебные заведения обязаны предоставить возможность получения качественного образования людям с ограниченными возможностями здоровья»*. Для слабовидящих и незрячих людей важным этапом является адаптация ресурсов обучения к возможностям пользователей [4, 10, 12].

Графический интерфейс электронных информационных ресурсов основан на визуальном восприятии информации и непригоден для людей, посещающих их через программу экранного доступа. И даже сайты, созданные с соблюдением стандартов по адаптации интернет-ресурсов для пользователей с проблемами зрения, не всегда удовлетворяют всем потребностям слабовидящих и незрячих, так как развитие общего программного обеспечения (ПО) опережает развитие специального ПО для людей с патологиями зрения. Эти проблемы имеют интернациональный характер [1, 2, 14].

Большинство электронных информационных ресурсов могут использоваться слабовидящими и незрячими пользователями только через специальные программы, такие, как программа чтения с экрана и программа увеличения шрифта. Работа с обеими программами вызывает трудности, так как в поле зрения попадает ограниченная часть экрана. Это осложняет восприятие материала. Анализ предметной области показал, что у слабовидящих и незрячих пользователей существуют следующие проблемы работы с электронными информационными ресурсами [10, 11, 12, 13]:

- недоступность чата и открытого общения;
- выполнение заданий по времени невозможно для слабовидящих и незрячих;
- наличие капчей (CAPTCHA, Completely Automated Public Turing test to tell Computers and Humans Apart — название тестов для отсеивания ботов);
- отсутствие комментариев к картинкам;
- размещение в веб-ресурсах различных неподписанных объектов;
- размещение материалов в виде pdf-файлов;
- обновление системы.

С учетом применения всех средств адаптации структурная модель работы незрячего пользователя, представленная на рис. 1, трансформируется в модель процесса адаптации электронных информационных ресурсов к потребностям слабовидящих и незрячих пользователей, представленную на рис. 3.

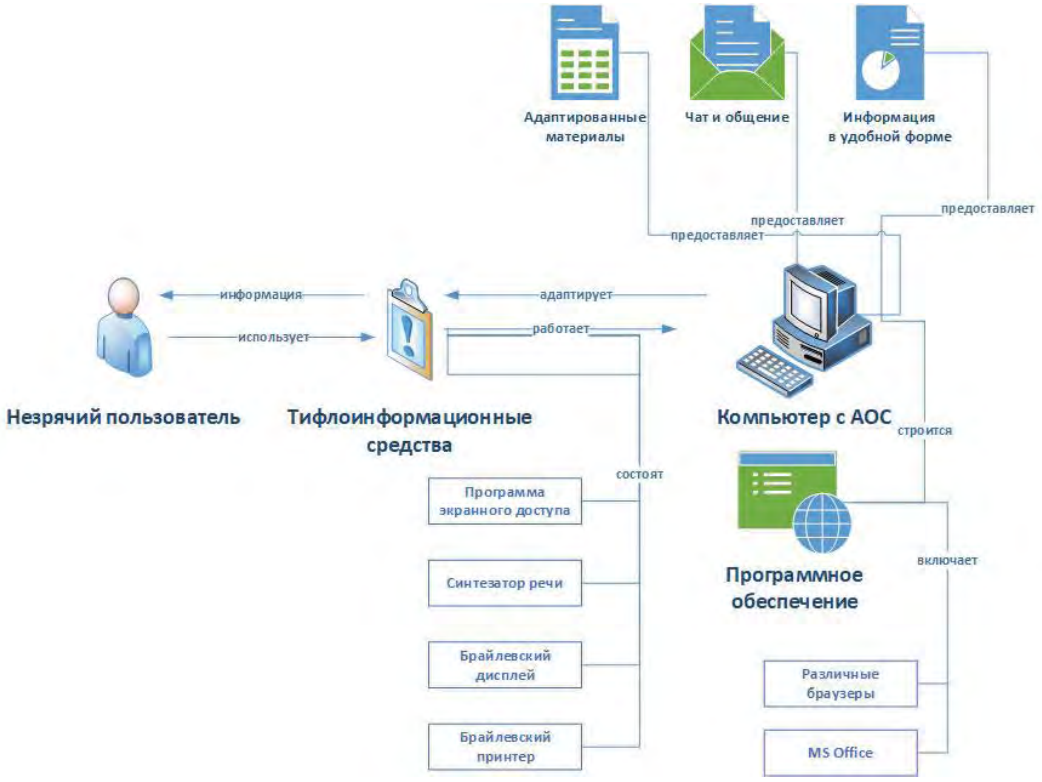

Рис. 3. Модель процесса адаптации ЭИР к потребностям слабовидящих и незрячих пользователей

Модель отражает все необходимые для слабовидящих и незрячих пользователей технические и программные средства, а также вид представления материалов.

Для обеспечения минимального доступа к электронным информационным ресурсам все они должны быть выполнены согласно ГОСТ Р 52872-2019[2]. На основании данного ГОСТа для разработки интернет-ресурсов, доступных инвалидам по зрению, необходимо соблюдать следующие основные принципы представления информации: воспринимаемость; управляемость; понятность; надежность.

Определение направлений решения проблем доступности ЭИР для слабовидящих и незрячих пользователей

Для понимания всех основных проблем использования современных электронных информационных ресурсов проведено *экспериментальное исследование* (с учетом [3]) среди слабовидящих и незрячих пользователей. Исследование проводилось на добровольной основе при помощи разработанных анкет, позволяющих выбрать варианты ответа или предложить свой вариант. В опросах приняли участие более 100 человек, период проведения исследования — 2019 год.

Анкета составлена таким образом, чтобы охарактеризовать: знания основ компьютерной грамотности; использование различных ресурсов; знания по дистанционному обучению слабовидящих и незрячих; осведомленность о применении в обучении специальных технических и программных средств; возможность работы людей с нарушениями зрения за компьютером. При анализе полученных данных использовался автоматический вывод результатов.

Целью данного исследования являлось определение основных информационных технологий для работы незрячего пользователя с персональным компьютером и выявление основных проблем в процессе работы с ЭИР.

Основные *задачи* исследования заключались в анализе данных, собранных при помощи опросов в виде анкет. Получены результаты опросов различных групп слабовидящих и незрячих пользователей, а также их окружения.

Для разработки опросов применялись технологии *Google Forms*. Их использование обусловлено, прежде всего, доступностью для людей с проблемами зрения. Созданные анкеты и опросы полностью управляемы при помощи обычной клавиатуры. Для корректной работы опроса каждый вопрос подписан и добавлены пояснения к нему: что необходимо выбрать, например, один или несколько вариантов ответа, обязателен ли этот вопрос и др. В этом случае будут соблюдены требования ГОСТ Р 52872-2019.

[2] ГОСТ Р 52872-2019. Интернет-ресурсы и другая информация, представленная в электронно-цифровой форме. Приложения для стационарных и мобильных устройств, иные пользовательские интерфейсы. Требования доступности для людей с инвалидностью и других лиц с ограничениями жизнедеятельности. М. : Стандартинформ, 2019. 37 с.

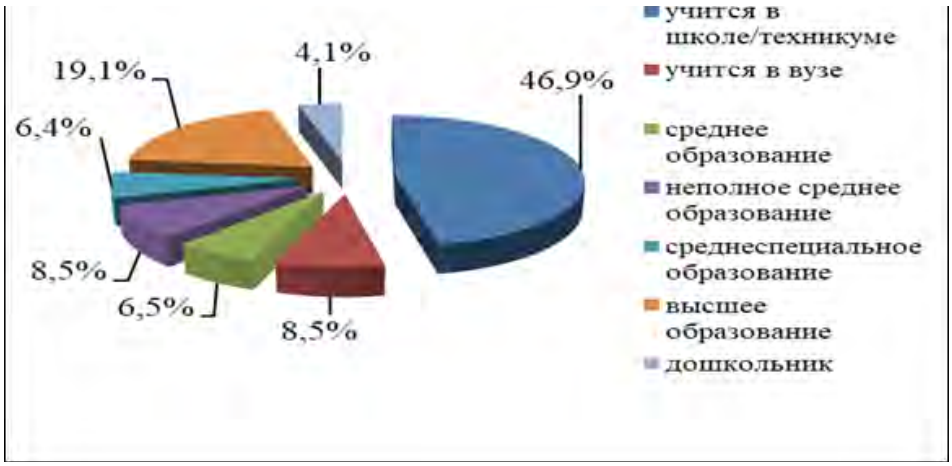

Рис. 4. Уровень образования респондентов

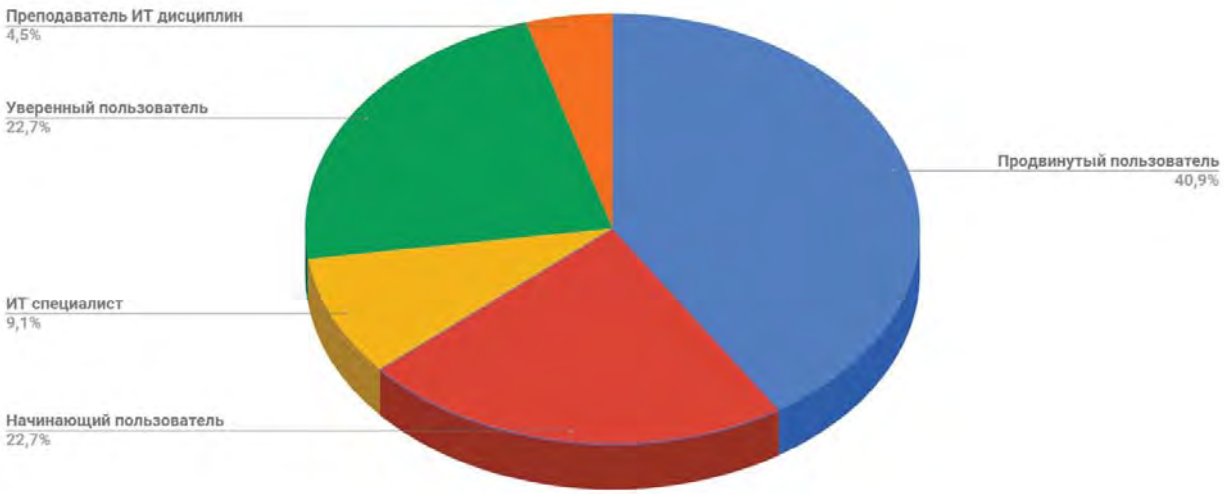

Рис. 5. Уровень компьютерной грамотности респондентов

В исследовании использовалась целевая *вероятностная* выборка. Из генеральной совокупности случайным образом предполагался отбор слабовидящих и незрячих респондентов разнообразных социальных групп и сообществ путем рассылки приглашений для участия в онлайн-опросе и размещения ссылки в социальных сетях на онлайн-анкетирование. То есть использовался так называемый «метод самоотбора».

Большая часть опрошенных — незрячие пользователи, в достаточной мере владеющие персональным компьютером. Более 50% имеют высшее или среднее специальное образование (рис. 4). Часть из них учащиеся (примерно 20%), бóльшая часть — работающее население (примерно 60%, около 10% из них фрилансеры) и небольшая часть — безработные (около 20%).

По уровню компьютерной грамотности 22% респондентов — начинающие пользователи, еще 22% — уверенные пользователи, 41% — продвинутые пользователи (установка и настройка ПО), 9% являются ИТ-специалистами и лишь небольшой процент опрошенных в самом начале изучения основ компьютерной грамотности или не используют компьютер. Такие показатели обусловлены тем, что выборка изначально проводилась среди пользователей сети Интернет (рис. 5).

Среди интересов в сети большинство респондентов выделяют общение в социальных сетях, поиск новой информации, обучение через Интернет и развлечения (рис. 6). Почти 50% опрошенных ищут знакомства в сети. Игры для слабовидящих и незрячих также распространены (более 36%).

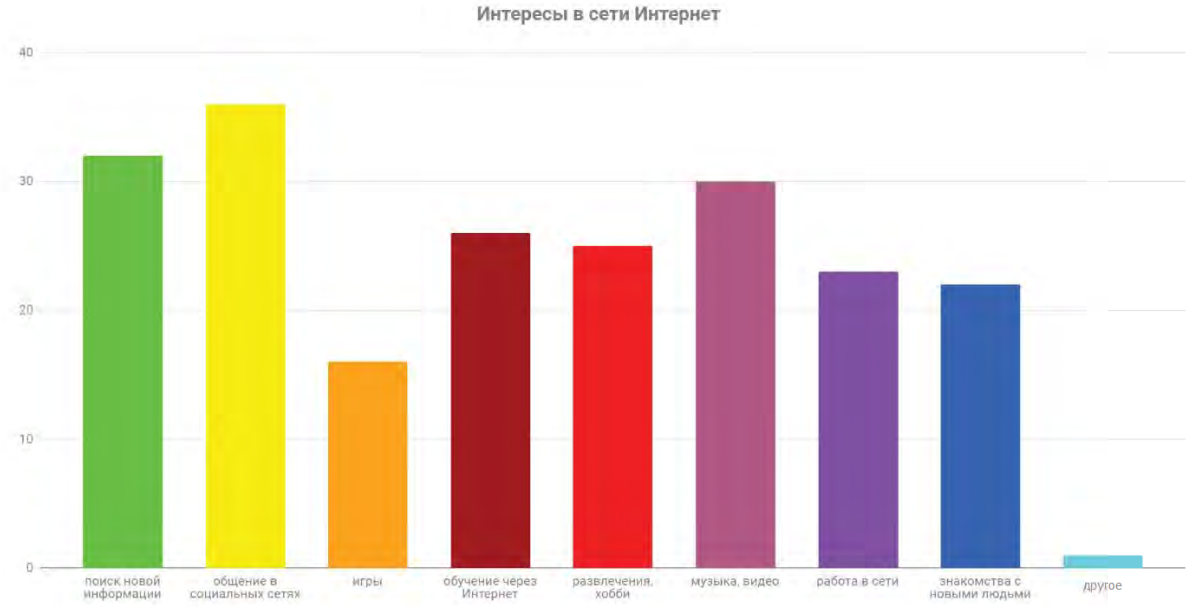

Рис. 6. Интересы в сети Интернет

На следующей диаграмме представлены данные опроса по пункту *«дистанционное обучение»*. Почти 22% респондентов учатся, используя различные системы дистанционного обучения. Более 33% опрошенных ищут в сети книги и учебники в аудио-формате или читаемые программой экранного доступа. Поиск информации и обучение при помощи ее практикуют 43,5% слабовидящих и незрячих (рис. 7).

Популярность программ экранного доступа представлена на рис. 8.

Из данных опроса видно, что большая часть респондентов использует программы экранного доступа *Jaws* и *NVDA*, позволяющие воспроизводить информацию с экрана монитора. Многие также выходят в сеть с мобильных устройств, используя установленные на них программы экранного доступа.

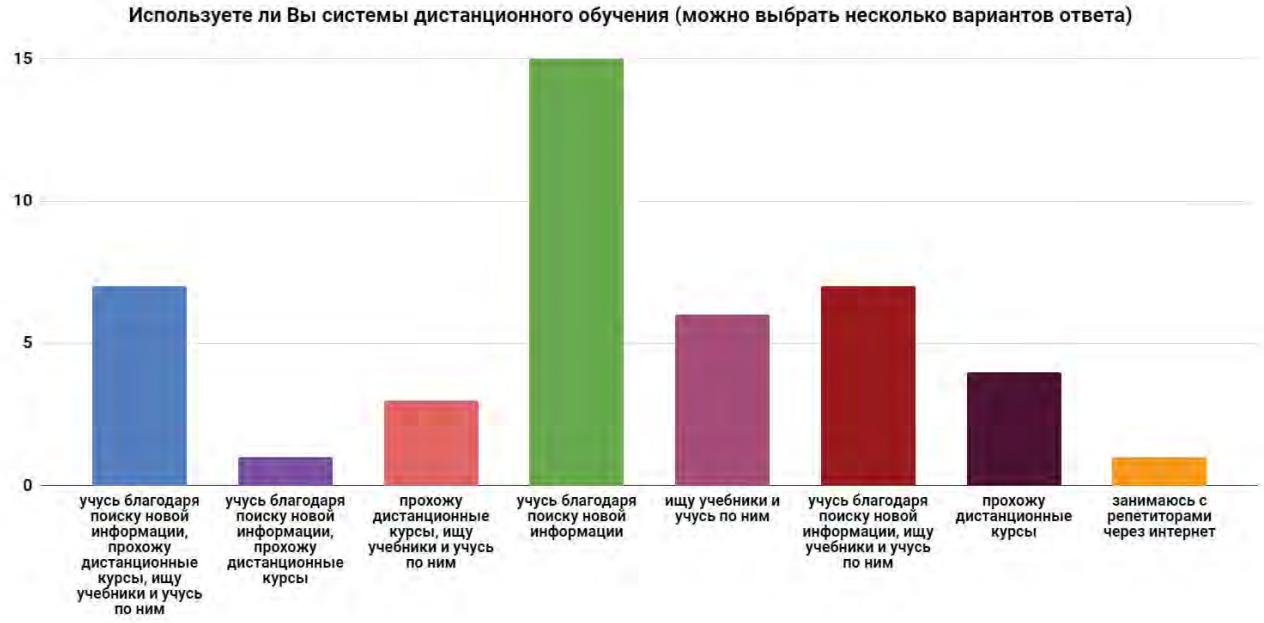

Рис. 7. Использование систем дистанционного обучения

Следующий вопрос анкеты касался доступности электронных информационных ресурсов в целом. Весь интерфейс компьютера ориентирован на зрительное восприятие информации, и часть проблем незрячих пользователей связана с этим. Разгадывание капчей, загрузка видео на странице сайта, неграмотная верстка, не учитывающая особенности программ чтения с экрана, делают работу затруднительной.

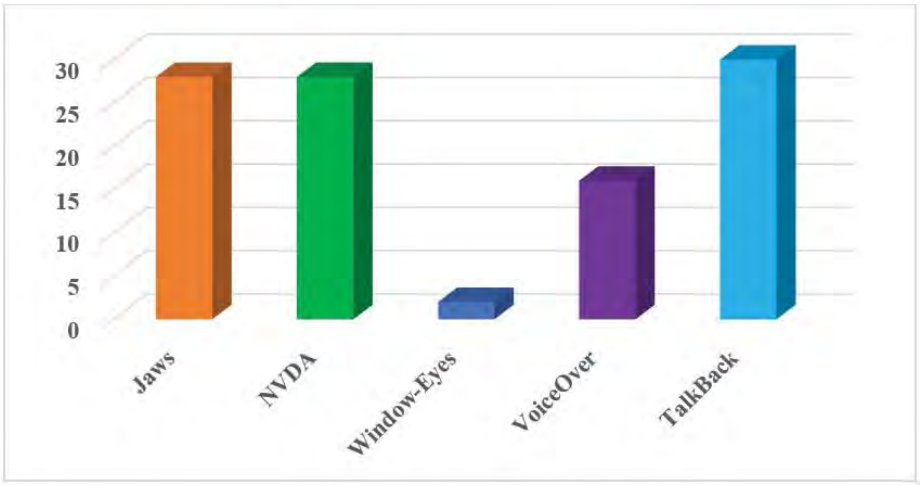

Рис. 8. Основные коммерческие программы экранного доступа

Основные проблемы, связанные с доступностью электронных информационных ресурсов, представлены на рис. 9. В результате определения проблем доступности выявлены все основные проблемы ЭИР, требующие решения.

Для обеспечения минимального доступа к ЭИР все электронные информационные ресурсы должны быть выполнены согласно ГОСТ Р 52872-2019, в соответствии с которым адаптация ЭИР имеет следующие *обязательные* параметры.

Первой ступенью адаптации на большинстве интернет-ресурсов является добавление модуля для слабовидящих. Такой модуль оправдан, если он дает возможность настройки контрастности и цветовой гаммы. Увеличение шрифта возможно комбинациями клавиш.

Всю *HTML*-верстку необходимо строить четко с применением заголовков разных уровней, для перехода по ним горячими клавишами клавиатуры (обычная стандартная клавиатура).

Графический материал в ЭИР должен быть подписан для озвучивания программой экранного доступа. Необходимо описание всех видов графики, а также назначения кнопок и переходов, используемых в ресурсе.

Все документы в ЭИР должны быть в формате *.doc* или читаемом *.pdf*. Желательна структура в виде заголовков внутри файла для перехода к необходимому материалу при помощи горячих клавиш клавиатуры.

Тесты необходимо адаптировать для полного управления клавиатурой, к каждому тесту обязательно пояснение (например, незрячий не может самостоятельно определить, один вариант нужно выбрать или несколько).

Структура ЭИР должна быть строгой и однородной на всех страницах, нельзя менять местами расположение кнопок, переходов, документов и др.

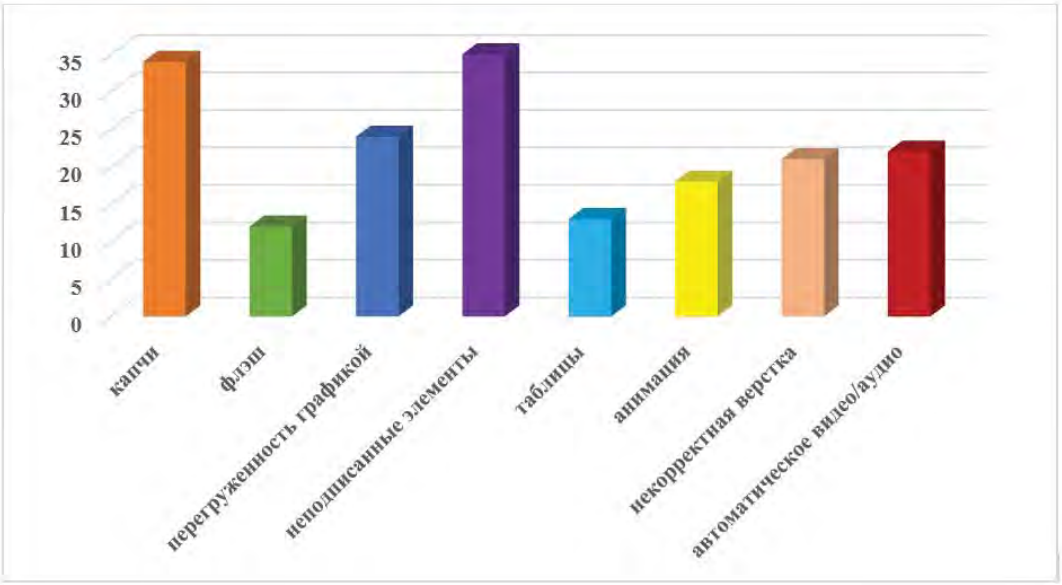

Рис. 9. Проблемы доступности интернет-ресурсов

Заключение

В настоящее время большинство электронных информационных ресурсов не полностью обеспечено правовым сопровождением процесса разработки программного обеспечения для обеспечения соблюдения ГОСТа. Системы дистанционного обучения, автоматизированные обучающие системы, сайты с полезной информацией, курсы повышения квалификации онлайн должны удовлетворять основным требованиям к адаптации электронных информационных ресурсов. Интерес пользователей к обучению и работе в сети растет, что обусловлено развитием информационных ресурсов в целом, поэтому изучение вопросов адаптации является важным для каждого разработчика и они должны соблюдать требования нормативно-правовой основы разработки электронных информационных ресурсов.

В результате исследования проблем адаптации электронных информационных ресурсов для слабовидящих и незрячих пользователей построена структурная модель работы незрячего пользователя, модель адаптации электронных информационных ресурсов для слабовидящих и незрячих пользователей и модель процесса адаптации ЭИР к потребностям слабовидящих и незрячих пользователей, дающие полное представление о процессе работы пользователей с проблемами зрения и вариантах решения проблем адаптации ЭИР.

На основе проведенного анализа определены пути решения проблем адаптации электронных информационных ресурсов для слабовидящих и незрячих пользователей.

Литература

1. Ардзинба В.А. Инклюзивное образование инвалидов в Соединенных Штатах Америки // Электронный журнал «Психологическая наука и образование». 2010. № 5. С. 23—29.
2. Бруштейн И. Незримая Германия. Путешествие в Марбург, «столицу немецких слепых» // Дефектология. 2011. № 6. С. 72—87.
3. Ващекин А.Н., Шевченко Д.И. Обмен информацией в профессиональной деятельности юриста: исследование особенностей коммуникативной деятельности // Правовая информатика. 2018. № 1. С. 23—31. DOI: 10.21681/1994-1404-2018-1-23-31 .
4. Денискина В.З. Особые образовательные потребности детей с нарушением зрения. Дефектология // Школьная пресса. 2012. № 6. С. 17—24.
5. Дубровина О.В., Чванова М.С. Адаптивные интернет-решения как катализатор развития системы открытого образования для людей со специальными потребностями // Труды Всеросс. науч.-прак. конф. «Образование. Технологии. Качество» (3 апреля 2017 г.) / СНИГУ им. Н.Г. Чернышевского. Саратов : Научная книга, 2017. С. 31—34.
6. Дубровина О.В. Исследование осведомленности людей об обучении слабовидящих и незрячих // Труды Междунар. науч.-прак. конф. «Актуальные проблемы информатики и информационных технологий» (7—8 сентября 2017 г.) / Тамбовский гос. ун-т им. Г. Р. Державина. Тамбов : ТГУ, 2017. С. 69—75.
7. Кукушкина О.И. Использование информационных технологий в различных областях специального образования : автореф. дис. ... док. пед. наук: 13.00.03. М., 2005. 58 с.
8. Ловцов Д.А. Информационная теория эргасистем. Тезаурус : монография. М. : Наука, 2005. 248 с. ISBN 5-02-033779-X.
9. Ловцов Д.А. Системный анализ. Часть. 1. Теоретические основы. М. : Рос. гос. ун-т правосудия, 2018. 224 с. ISBN 978-5-93916-701-7.
10. Рощина М.А. Основы компьютерных тифлотехнологий. Н. Новгород : ЦСТПР «Камерата», 2007. С. 60.
11. Рощина М.А. Проблемы тифлокомпьютеризации в России // Наша жизнь. 2005. № 53. С. 12—18.
12. Чванова М.С., Дубровина О.В. Особенности социализации слабовидящих и незрячих в процессе обучения в Германии, Франции и США // Профессиональное образование в России и за рубежом. 2018. № 4(32). С. 222—231.
13. Швецов В.И., Рощина М.А. Компьютерные тифлотехнологии в социальной интеграции лиц с глубокими нарушениями зрения. Н. Новгород : Нижегородский гос. ун-т, 2007. 154 с.
14. Т-технологии как средство реабилитации незрячих людей: состояние, проблемы и перспективы // Труды Всеросс. науч.-прак. конф. (30 ноября — 2 декабря 2011 г.) / Пермская краевая специальная библиотека для слепых. Пермь, 2011. 152 с.

Рецензент: ***Бетанов Владимир Вадимович,*** *доктор технических наук, профессор, член-корреспондент РАРАН, начальник центра АО «Российские космические системы», г. Москва.*
E-mail: vlavab@mail.ru

ELECTRONIC INFORMATION RESOURCES ADAPTATION MODELLING FOR VISUALLY IMPAIRED AND BLIND USERS

Vladimir Alekseev, *Dr.Sc. (Technology), Professor, Head of the Information Systems and Information Protection Department of the Tambov State Technical University, Tambov, Russian Federation.*
E-mail: vvalex1961@yandex.ru

Oksana Dubrovina, *Ph.D. student at the Information Systems and Information Protection Department of the Tambov State Technical University, Tambov, Russian Federation.*
E-mail: prepov@rambler.ru

Keywords: *electronic information resources, non-visual access, braille display, braille printer, screen reader, speech synthesisers, information tools and technologies for the blind and visually impaired.*

Abstract.

Purpose of the paper: identifying and determining ways for solving problems limiting the opportunities of visually impaired and blind users to access electronic information resources.

Methods used: informational and legal analysis, conceptual and logical modelling, quantitative analysis, self-selection method.

Results obtained: the main problems of access of visually impaired and blind users to electronic information resources were identified, mechanisms and means needed for access to electronic information resources were studied, models of work and adaptation of electronic information resources to the needs of visually impaired and blind users were developed, and ways for solving problematic issues of access of visually impaired and blind users to electronic information resources were determined.

References

1. Ardzinba V.A. Inkliuzivnoe obrazovanie invalidov v Soedinennykh Shtatakh Ameriki. Elektronnyi zhurnal "Psikhologicheskaia nauka i obrazovanie", 2010, No. 5, pp. 23-29.
2. Brushtein I. Nezrimaia Germaniia. Puteshestvie v Marburg, "stolitsu nemetskikh slepykh". Defektologiia, 2011, No. 6, pp. 72-87.
3. Vashchekin A.N., Shevchenko D.I. Obmen informatsiei v professional'noi deiatel'nosti iurista: issledovanie osobennostei kommunikativnoi deiatel'nosti. Pravovaia informatika, 2018, No. 1, pp. 23-31. DOI: 10.21681/1994-1404-2018-1-23-31 .
4. Deniskina V.Z. Osobye obrazovatel'nye potrebnosti detei s narusheniem zreniia. Defektologiia. Shkol'naia pressa, 2012, No. 6, pp. 17-24.
5. Dubrovina O.V., Chvanova M.S. Adaptivnye internet-resheniia kak katalizator razvitiia sistemy otkrytogo obrazovaniia dlia liudei so spetsial'nymi potrebnostiami. Trudy Vseross. nauch.-prak. konf. "Obrazovanie. Tekhnologii. Kachestvo" (3 aprelia 2017 g.), SNIGU im. N.G. Chernyshevskogo. Saratov : Nauchnaia kniga, 2017, pp. 31-34.
6. Dubrovina O.V. Issledovanie osvedomlennosti liudei ob obuchenii slabovidiashchikh i nezriachikh. Trudy Mezhdunar. nauch.-prak. konf. "Aktual'nye problemy informatiki i informatsionnykh tekhnologii" (7-8 sentiabria 2017 g.), Tambovskii gos. un-t im. G. R. Derzhavina. Tambov : TGU, 2017, pp. 69-75.
7. Kukushkina O. I. Ispol'zovanie informatsionnykh tekhnologii v razlichnykh oblastiakh spetsial'nogo obrazovaniia : avtoref. dis. ... dok. ped. nauk: 13.00.03. M., 2005. 58 pp.
8. Lovtsov D.A. Informatsionnaia teoriia ergasistem. Tezaurus : monografiia. M. : Nauka, 2005. 248 c. ISBN 5-02-033779-X.
9. Lovtsov D.A. Sistemnyi analiz. Chast'. 1. Teoreticheskie osnovy. M. : Ros. gos. un-t pravosudiia, 2018. 224 pp. ISBN 978-5-93916-701-7.
10. Roshchina M.A. Osnovy komp'iuternykh tiflotekhnologii. N. Novgorod : TsSTPR "Kamerata", 2007, pp. 60.
11. Roshchina M.A. Problemy tiflokomp'iuterizatsii v Rossii. Nasha zhizn', 2005, No. 53, pp. 12-18.
12. Chvanova M.S., Dubrovina O.V. Osobennosti sotsializatsii slabovidiashchikh i nezriachikh v protsesse obucheniia v Germanii, Frantsii i SShA. Professional'noe obrazovanie v Rossii i za rubezhom, 2018, No. 4(32), pp. 222-231.
13. Shvetsov V.I., Roshchina M.A. Komp'iuternye tiflotekhnologii v sotsial'noi integratsii lits s glubokimi narusheniiami zreniia. N. Novgorod : Nizhegorodskii gos. un-t, 2007. 154 pp.
14. IT-tekhnologii kak sredstvo reabilitatsii nezriachikh liudei: sostoianie, problemy i perspektivy. Trudy Vseross. nauch.-prak. konf. (30 noiabria -- 2 dekabria 2011 g.). Permskaia kraevaia spetsial'naia biblioteka dlia slepykh. Perm', 2011. 152 pp.