ISSN 2518-1092

НАУЧНЫЙ РЕЗУЛЬТАТ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

RESEARCH RESULT. INFORMATION TECHNOLOGY

Том 5 № 3
Volume 5 2020

16+

Сайт журнала:
rrinformation.ru
сетевой научный рецензируемый журнал
online scholarly peer-reviewed journal

НАУЧНЫЙ РЕЗУЛЬТАТ
RESEARCH RESULT

НАУЧНЫЙ РЕЗУЛЬТАТ. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
RESEARCH RESULT. INFORMATION TECHNOLOGIES

Журнал зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)
Свидетельство о регистрации средства массовой информации Эл. № ФС77-69101 от 14 марта 2017 г.

The journal has been registered at the Federal service for supervision of communications information technology and mass media (Roskomnadzor)
Mass media registration certificate El. № FS 77-69101 of March 14, 2017

Том 5, № 3. 2020

Volume 5, № 3. 2020

СЕТЕВОЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ
Издается с 2016 г.
ISSN 2518-1092

ONLINESCHOLARLYPEER-REVIEWEDJOURNAL
First published online: 2016
ISSN 2518-1092

Учредитель: Федеральное государственное автономное образовательное учреждение высшего образования «Белгородский государственный национальный исследовательский университет»
Издатель: НИУ «БелГУ». Адрес издателя: 308015 г. Белгород, ул. Победы, 85.
Журнал выходит 4 раза в год

Founder: Federal state autonomous educational establishment of higher education «Belgorod State National Research University»
Publisher: Belgorod State National Research University
Address of publisher: 85 Pobeda St., Belgorod, 308015, Russia
Publication frequency: 4 /year

СОДЕРЖАНИЕ

CONTENTS

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

INFORMATION SYSTEM AND TECHNOLOGIES

АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ

AUTOMATION AND CONTROL

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ
INFORMATION SYSTEM AND TECHNOLOGIES

УДК 004.491 **DOI: 10.18413/2518-1092-2020-5-3-0-1**

Гоголь А.С.
Маслова М.А.

ОСНОВНЫЕ ВИДЫ КОМПЬЮТЕРНЫХ УГРОЗ

Севастопольский государственный университет, ул. Университетская, д. 33, г. Севастополь, 299053, Россия

e-mail: andrey.gogol.99@mail.ru, info@sevsu.ru, machechka-81@mail.ru

Аннотация
Компьютер – устройство, созданное для выполнения на данном устройстве операций. Данные операции определяются и задаются пользователем, и эти последовательности операций называют программами. Чаще всего это математические расчеты, но к этим последовательностям можно относить и операции ввода данных и их вывода. Сегодня люди объединяют компьютеры и получают из них сети и системы с огромным множеством таких инструкций. В наше время практически у каждого человека имеется портативный компьютер, с которым он путешествует, с помощью которого он обменивается данными с друзьями, коллегами либо родными. Пользователи данных устройств обмениваются данными друг с другом по сети «Интернет» и не только. Так же они создают локальные сети для обеспечения внутреннего электронного документооборота на предприятии. Либо передают информацию посредством внешних накопителей. Учитывая, уровень информатизации и масштабы информационной инфраструктуры, можно понять, что существует немало уязвимостей. Используя данные уязвимости, любой злоумышленник может внедрить вредоносное программное обеспечение в наш компьютер. Цель статьи – провести анализ существующих видов компьютерных угроз, проанализировать уязвимости и составить рекомендации, которые позволят избежать нарушений в работе системы.
Ключевые слова: компьютерные программы; компьютерные угрозы; уязвимости; вредоносное программное обеспечение; информация.

UDC 004.491

Gogol A.S.
Maslova M.A.

MAIN TYPES OF COMPUTER THREATS

Sevastopol state University, 33 Universitetskaya St., Sevastopol, 299053, Russia

e-mail: andrey.gogol.99@mail.ru, info@sevsu.ru, machechka-81@mail.ru

Abstract
Computer – a device created for performing operations on this device. These operations are defined and specified by the user, and these sequences of operations are called programs. Most often these are mathematical calculations, but these sequences can also include data entry and output operations. Today, people combine computers and get networks and systems from them with a huge number of such instructions. Nowadays, almost every person has a portable computer with which they travel, with which they exchange data with friends, colleagues or relatives. Users of these devices exchange data with each other over the Internet and beyond. They also create local networks to ensure internal electronic document management at the enterprise. Or transmit information via external storage devices. Given the level of Informatization and the scale of the information infrastructure, we can understand that there are many vulnerabilities. Using these vulnerabilities, any attacker can inject malicious software into our computer. The purpose of the

article is to analyze existing types of computer threats, analyze vulnerabilities, and make recommendations that will help avoid system failures.
Keywords: computer programs; computer threats; vulnerabilities; malicious software; information.

ВВЕДЕНИЕ

Проведем анализ актуальных компьютерных угроз. При анализе компьютерных угроз необходимо помнить и о неопытности либо о неосведомленность пользователя. Пользователь и сам может скачать вредоносное программное обеспечение, которое через любой промежуток времени нарушит любое свойство информации. Человеческий фактор, является самой распространенной уязвимостью, которую злоумышленники успешно используют сегодня, тем самым нарушая конфиденциальность, целостность и доступность информации. Из-за доступных уязвимостей многие компании и иногда рядовые пользователи несут огромные финансовые убытки. Эти проблемы будут актуальны всегда, пока существует и хранится информация, которая имеет определенную ценность. При всём этом любой другой пользователь может потерять персональные данные, которые хранятся на его персональном компьютере либо на мобильном устройстве. Чаще всего вредоносное программное обеспечение не выбирает какую-либо определенную организацию, либо человека.

ОСНОВНАЯ ЧАСТЬ

Рассмотрим основные виды компьютерных угроз, существующих сегодня (Рисунок 1).

Вирус либо программа-троянец находятся в интернете и распространяются столько, сколько потребуется. Данное программное обеспечение может годами быть неактивным и просто ожидать. Например, вредоносная программа-троянец «Petya» в июне 2017 года распространилась по множеству стран мира и поразила огромное количество компьютеров. Сети больших нефтяных компаний и обычные медицинские лаборатории лишились информации, которая хранилась на их стационарных компьютерах. Данный вирус можно назвать не только троянским программным обеспечением, но и шифровальщиком. Он переписывал главные загрузочные записи пользователей операционной системы Microsoft Windows и после этого шифровал базы данных, в которых хранились сведения о содержимом тома с файловой системой [1].

Таким образом, пользователь терял доступ к операционной системе и данным, которые находились на носителях. Пользователю предлагалось купить ключ, который разблокирует его операционную систему.

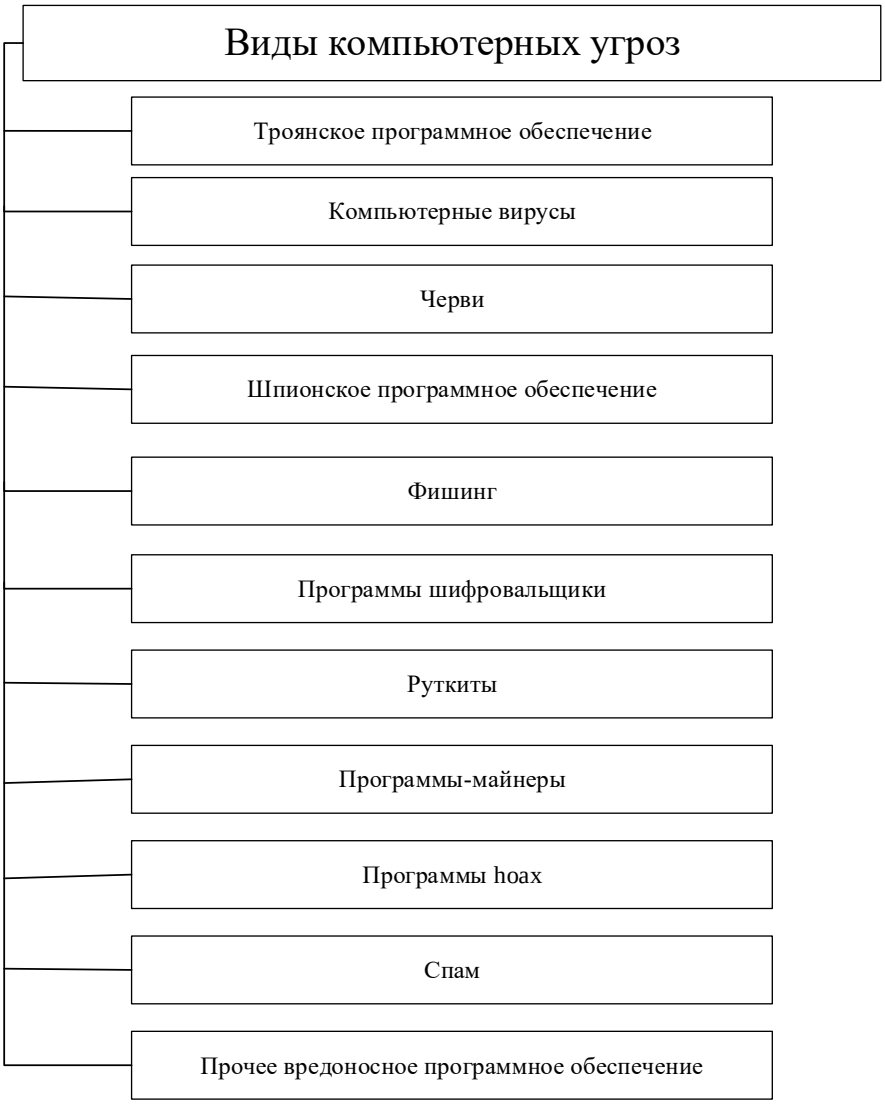

Рис. 1. Основные виды компьютерных угроз
Fig. 1. Main types of computer threats

Через некоторое время у вируса «Petya» появился помощник «Misha», который вступал в действие при неудачной попытке блокировки вирусом «Petya». Вирус «Misha», в свою очередь, блокировал .exe файлы и никак не затрагивал системные файлы. Пользователь входил в операционную систему и не мог использовать программы. По данным компании Касперский самый большой процент атак выдался на Украину и Россию из-за стремительного распространения данного вируса в системе для электронного документооборота компании M.E.Doc на территории Украины [9].

Таблица 1

Процентное соотношение заражения стран мира по данным Kaspersky.Lab

Table 1

Percentage of infection in countries of the world according to Kaspersky.Lab data

Страна	**Процент заражения**
Украина	60.0%
Россия	31.1%
Польша	6.0%
Италия	4.0%
Германия	2.0%
Беларусь	0.09%

После улучшения вирус распространился на другие государства и в большей степени от него пострадали крупные компании.

Таблица 2

Количество зафиксированных и отраженных атак за первое полугодие 2018 года по данным Kaspersky.Lab

Table 2

Number of recorded and repelled attacks for the first half of 2018 according to Kaspersky.Lab data

Вид отраженной атаки	**Количество атак/пользователей**
Веб-атака вредоносного программного обеспечения	243 749 050
Уникальные вредоносные зафиксированные URL	65 559 498
Пользователи, на компьютерах которых отражены атаки шифровальщиков	80 901
Пользователей, на компьютерах которых отражены атаки с использованием программ-майнеров	1 362 123

За годы развития информационной инфраструктуры злоумышленники придумали огромное количество разновидностей вредоносного программного обеспечения.

Сегодня каждая угроза может использоваться в связке с другой угрозой. Например, пользователь получает спам, читает сообщение и переходит по ссылке. Данное сообщение содержит такую информацию, которая определенно заинтересует данного пользователя и сыграет на его любопытстве. Далее пользователь переходит по ссылке либо скачивает вредоносный файл, и это вредоносное программное обеспечение в виде троянца начнёт действовать на его компьютере. Таким образом, будет нарушена доступность, целостность и конфиденциальность информации, которая хранится на данном устройстве. И мы получаем связку из трех и более угроз для компьютера, в которую входят: спам, фишинг, троянское программное обеспечение. Вместо троянского программного обеспечения может быть, любой другой вид компьютерной угрозы [4].

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ИХ ОБСУЖДЕНИЕ

По данным лаборатории Касперского можно сгруппировать угрозы на три вида (Таблица 3).

Таблица 3

Данные из пирамиды киберугроз Kaspersky.Lab за 2018 г.

Table 3

Data from the Kaspersky cyber threat pyramid.Lab for 2018

Название вида	**Процент**
Кибероружие: уникальные угрозы	0,1%
Целевые атаки: изощренные угрозы	9,9%
Массовые атаки	90%

Можно понять, что большая часть атак – это массовые атаки, такие как вирус-шифровальщик «Petya».

Рассмотрим отдельно каждый из видов угроз:

1) Троянское программное обеспечение – вредоносное программное обеспечение, которое выполняет несанкционированное уничтожение файлов как системных, так и обычных приложений. Данные программы нарушают не только доступность к информации, но и целостность, конфиденциальность.

Данная угроза не похожа на червей либо вирусы, так как она не имеет свойство распространения на другие компьютеры, но попадая в систему, она может нанести системе огромный вред [6].

2) Компьютерные вирусы – программы, внедряющие вредоносные инструкции в любое программное обеспечение пользователя. Они были придуманы для распространения, и при этом распространении они стирают и изменяют файлы.

3) Черви – вредоносный код, который при своем распространении использует ресурсы сети. Отсюда и пошло это название. Так как черви имеют способность «ползти» из одного компьютера к другому по каналам связи. [7]

Черви распространяются с более высокой скоростью. Они обнаруживают IP-адреса других компьютеров и распространяются по ним. Иногда они могут воспользоваться лишь оперативной памятью компьютера. [2]

4) Шпионское программное обеспечение – программы, которые несанкционированно и целенаправленно собирают сведения о пользователе. Они могут быть скрыты и пользователь не узнает об их присутствии до конца их работы. [10]

Данные программы могут производить сканирование жесткого диска и собирать информацию об установленном программном обеспечении. Также они могут собирать информацию о сетевых настройках устройства.

Существует шпионское программное обеспечение, которое при всем этом позволяет контролировать компьютер жертвы. Существуют встраиваемые в браузер программы, которые перенаправляют трафик. Так при запросе одного сайта пользователя направляют на другой.

5) Фишинг – вид социальной инженерии, при котором происходит «выуживание» каких-либо данных у пользователя. Использует письмо с текстом, который заинтересует пользователя, далее он переходит по вредоносной ссылке. Также человек может оставить свои логин и пароль на поддельном сайте. [3]

6) Руткиты – утилиты, которые используются для маскировки подозрительной активности на устройстве человека. Данные утилиты маскируют деятельность вирусов, червей и троянцев.

Также они могут изменять функции операционной системы тем самым, маскируя себя и злоумышленника.

7) Программы шифровальщики – программное обеспечение, которое при попадании на устройство рядового пользователя, шифрует ценные для него файлы, а иногда и системные. Если данная программа шифрует системные файлы, то пользователь теряет доступ ко всей операционной системе и данным. Чаще всего такие программы требуют выкуп.

8) Программы-майнеры – программы, которые без ведома человека начинают эксплуатацию ресурсов его компьютера для майнинга криптовалюты. Вся мощность компьютера уходит на майнинг и работает на злоумышленника. Чаще всего можно заметить как на персональном компьютере падает производительность

9) Ноах-программы – программное обеспечение, которое навязывает пользователю покупку другого продукта путем обмана. Например, она может выдать пользователю баннер, на котором будет написано, что компьютер подвергся атаке.

10) Спам – корреспонденция нежелательного характера, которая рассылается массово и может использоваться злоумышленниками для кражи данных либо для распространения зловредного программного-обеспечения. [8]

Так же не стоит забывать о других угрозах. Такие угрозы как программы, которые созданы для создания других вредоносных программ и их распространения, организованные DDOS атаки на сервера и другие зловредные утилиты и приложения. [5]

Для предотвращения некоторых из угроз рекомендуется:

1) обновлять своевременно, вручную базы данных антивируса;

2) не платить выкуп, так как вскоре ключ от программы шифровальщика выложат в открытый доступ, и никто не будет идти на поводу у злоумышленника;

3) устанавливать последние обновления операционной системы;

4) убедится, что включены все компоненты антивируса;

5) сделать резервное копирование файлов.

ЗАКЛЮЧЕНИЕ

Безусловно, компьютер стал частью жизни практически каждого жителя нашей планеты, за счёт высокого уровня информатизации. Проанализированные виды компьютерных угроз показывают, что возросло и количество злоумышленников и созданных ими зловредных программ. Данные программные обеспечение направлены на уничтожение, искажение, распространение данной информации. Некоторое программное обеспечение создано для того, чтобы вымогать денежные средства у человека. Для обеспечения собственной безопасности, либо безопасности компании создают антивирусные программы, которые отвечают всем требованиям и способны защитить пользователя в полной мере от всех имеющихся и появляющихся угроз. Но при всем этом не стоит забывать о том, что сам пользователь может совершить ошибку и пустить вредоносный код в свою систему, что может привести к непоправимому ущербу. Таким образом, необходимо периодически проводить анализ новых угроз, чтобы всегда быть во «всеоружии». Особенно это важно для руководителей компаний. Они должны интересоваться сами и при этом осведомлять своих сотрудников о всех имеющихся компьютерных угрозах своевременно.

Список литературы

1. Всё что нужно знать о новой эпидемии [Электронный ресурс] URL: https://xakep.ru/2017/06/28/petya-write-up/.
2. Гуляев В. Р., Струнькина В. А. Компьютерные вирусы – проблема XXI века // Юный ученый. – 2017. – №1. – С. 54-56. – URL https://moluch.ru/young/archive/10/752/.
3. Гуськова А. М. Фишинг как основной метод социальной инженерии в схемах финансового мошенничества [Текст] // Исследования молодых ученых: материалы III Междунар. науч. конф. (г. Казань, октябрь 2019 г.). – Казань: Молодой ученый, 2019. – С. 3-6. – URL https://moluch.ru/conf/stud/archive/349/15208/
4. Как работает фишинг [Электронный ресурс] URL: https://www.kaspersky.ru/blog/how-to-avoid-phishing/5411/.
5. Общие сведения о компьютерных угрозах [Электронный ресурс] URL: https://support.kaspersky.ru/614#block1.
6. Трубачёв Евгений Сергеевич Троянские программы: механизмы проникновения и заражения // Вестник ВУиТ. – 2011. – №18. – URL: https://cyberleninka.ru/article/n/troyanskie-programmy-mehanizmy-proniknoveniya-i-zarazheniya.
7. Что такое компьютерный вирус и компьютерный червь? [Электронный ресурс] URL: https://www.kaspersky.ru/resource-center/threats/viruses-worms.
8. Что такое спам? [Электронный ресурс] URL: https://encyclopedia.kaspersky.ru/knowledge/what-is-spam/.
9. Шифровальщик Petya/NotPetya/ExPetr [Электронный ресурс] URL: https://www.kaspersky.ru/blog/new-ransomware-epidemics/17855/.
10. Шпионские программы [Электронный ресурс] URL: https://ru.malwarebytes.com/spyware/.

References

1. Everything you need to know about the new epidemic [Electronic resource] URL: https://xakep.ru/2017/06/28/petya-write-up/.
2. Gulyaev V. R., Strunkina V. A. Computer viruses-the problem of the XXI century // Young scientist. – 2017. – no. 1. – P. 54-56. – URL https://moluch.ru/young/archive/10/752/.
3. Guskova a.m. Phishing as the main method of social engineering in financial fraud schemes [Text] // Research of young scientists: materials of the III international conference. scientific conference (Kazan, October 2019). – Kazan: Young scientist, 2019. – P. 3-6. – URL https://moluch.ru/conf/stud/archive/349/15208/.
4. How phishing works [Electronic resource] URL: https://www.kaspersky.ru/blog/how-to-avoid-phishing/5411/.
5. General information about computer threats [Electronic resource] URL: https://support.kaspersky.ru/614#block1.
6. Trubachev Evgeny Sergeevich Trojan programs: mechanisms of penetration and infection // Vestnik Vuit. – 2011. – №18. – URL: https://cyberleninka.ru/article/n/troyanskie-programmy-mehanizmy-proniknoveniya-i-zarazheniya.

7. What is a computer virus and a computer worm? [Electronic resource] URL: https://www.kaspersky.ru/resource-center/threats/viruses-worms.
8. What is spam? [Electronic resource] URL: https://encyclopedia.kaspersky.ru/knowledge/what-is-spam/.
9. cryptographer Petya/NotPetya/ExPetr [Electronic resource] URL: https://www.kaspersky.ru/blog/new-ransomware-epidemics/17855/.
10. Spy programs [Electronic resource]. URL: https://ru.malwarebytes.com/spyware/.

Гоголь Андрей Сергеевич, студент 4 курса кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности
Маслова Мария Александровна, аспирант, старший преподаватель кафедры «Информационная безопасность» Института радиоэлектроники и информационной безопасности

Gogol Andrey Sergeevich, 4th year student of the Department Information security, Institute of Radioelectronics and Information security
Maslova Maria Alexandrovna, post-graduate student, senior lecturer of the Department «Information security», Institute of Radioelectronics and Information security

УДК 004 **DOI: 10.18413/2518-1092-2020-5-3-0-2**

Шевцов М.
Маслова М.А.

ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ СИСТЕМ ЦИФРОВОЙ НАЛИЧНОСТИ

Севастопольский государственный университет, ул. Университетская, д. 33, г. Севастополь, 299053, Россия

e-mail: maxim.sevtov@gmail.com, info@sevsu.ru, machechka-81@mail.ru

Аннотация
С развитием информационных технологий все большую популярность приобретают системы цифровой (электронной) наличности. Перед обычными денежными знаками цифровая наличность обладает рядом преимуществ, и количество преимуществ растет по мере того, как информационные технологии интегрируются в общественную жизнь.
Целью исследования является выделение преимуществ систем цифровой наличности перед обычными денежными знаками; провести классификацию различных видов цифровой наличности; сравнение существующих систем электронной валюты, и выявление уязвимостей современных систем цифровой наличности. Сравнение различных систем проводится по таким критериям, как возможность работы без связи с серверами, разновидности способов подтверждения подлинности, способам защиты от копирования, и т. д. По окончанию исследования, можно будет сделать выводы касаемо готовности мира к массовому переходу на системы цифровой наличности, о преимуществах и недостатках того или иного вида электронной наличности, выделить уязвимости в современных видах электронной наличности, а также сделать прогноз на развитие цифровой наличности в будущем.
Ключевые слова: цифровая наличность; криптовалюта; информационная безопасность; валюта; криптозащита; Bitcoin.

UDC 004

Shevtsov M.
Maslova M.A.

RESEARCH OF THE SECURITY OF MODERN DIGITAL CASH SYSTEMS

Sevastopol state University, 33 Universitetskaya St., Sevastopol, 299053, Russia

e-mail: maxim.sevtov@gmail.com, info@sevsu.ru, machechka-81@mail.ru

Abstract
With the development of information technology, digital (electronic) cash systems are becoming increasingly popular. Digital cash has a number of advantages over conventional currency, and the number of advantages grows as information technology is integrated into public life.
The aim of the study is to highlight the advantages of digital cash systems over conventional banknotes, provide a classification of various types of digital cash, compare existing electronic currency systems, and identify the vulnerabilities of modern digital cash systems. Comparison of various systems is carried out according to such criteria as the ability to work without communication with servers, a variety of authentication methods, copy protection methods, etc.
At the end of the research, it will be possible to draw conclusions regarding the world's readiness for a massive transition to digital cash systems, the advantages and disadvantages of this or that type of electronic cash, highlight vulnerabilities in modern types of electronic cash, and make a forecast for the development of digital cash in the future.
Keywords: digital cash; cryptocurrency; information security; currency; crypto protection, Bitcoin.

ВВЕДЕНИЕ

Несмотря на высокий уровень развития информационных технологий, их все более глубокое внедрение во все области человеческой деятельности, нельзя сделать вывод, что

цифровые деньги вот-вот вытеснят обычную валюту. Этому мешает и длительный опыт работы с привычными всем денежными знаками, так и недоверие к электронной валюте как со стороны обычных людей, так и со стороны государств. Во многих странах Центробанки все ещё очень настороженно относятся к наличию электронных денег. Также, нет определенного правового регулирования цифровой наличности, ибо многие государства все ещё не определились в своем отношении к цифровой валюте.

Немаловажным фактором торможения внедрения электронной наличности является слабые познания в безопасности таких систем. Исследование безопасности таких систем и является целью этого исследования. Дать ответ на вопрос, насколько безопасней использование цифровой наличности, сложней оттого, что история использования цифровой валюты достаточно коротка, и методы её реализации зачастую рознятся от типа рассматриваемой криптовалюты. Тот факт, что методы защиты валюты постоянно совершенствуются и меняются, также затрудняет изучение это вопроса.

Цель исследования: безопасность современных систем цифровой наличности.

Объект исследования: цифровая наличность.

Итогом исследования будет изучение уязвимостей различных систем цифровой наличности, что позволит дать ответ на то, какой из видов цифровой валюты на сегодняшний день наиболее перспективен, а также понять, готовы ли системы цифровой наличности прийти на смену привычным всем денежным знакам [7].

ОСНОВНАЯ ЧАСТЬ

В качестве входных материалов используются преимущества и недостатки обычных денежных знаков, что, в сравнении с цифровой наличностью, даст ответ на вопрос, стоит ли стремится к замене обычной наличности цифровыми деньгами [5].

Также, следует привести классификацию электронной наличности, выделить уязвимости каждой из них, и выполнить их сравнение, по таким вопросам, как: возможность работать в режиме off-line, способы подтверждения личности, способы защиты от копирования. Классификация электронных денег приведена на рисунке 1. [10]

Электронные деньги можно разделить на две категории: те, что построены на базе смарт-карт, и те, что на базе сетей. Так же, их можно разделить на фиатные и нефиатные. Фиатные деньги выражены в государственной валюте. Обращение таких денег происходит по всем тем правилам, что диктуют государства, Центробанки, и т.д. Нефиатные деньги используют свои платежные системы. Они могут быть привязаны к какой-либо валюте, однако, государство не гарантирует их ценность и надежность. Соответственно, и регулирование таких систем со стороны государства отлично от фиатных [7], [8].

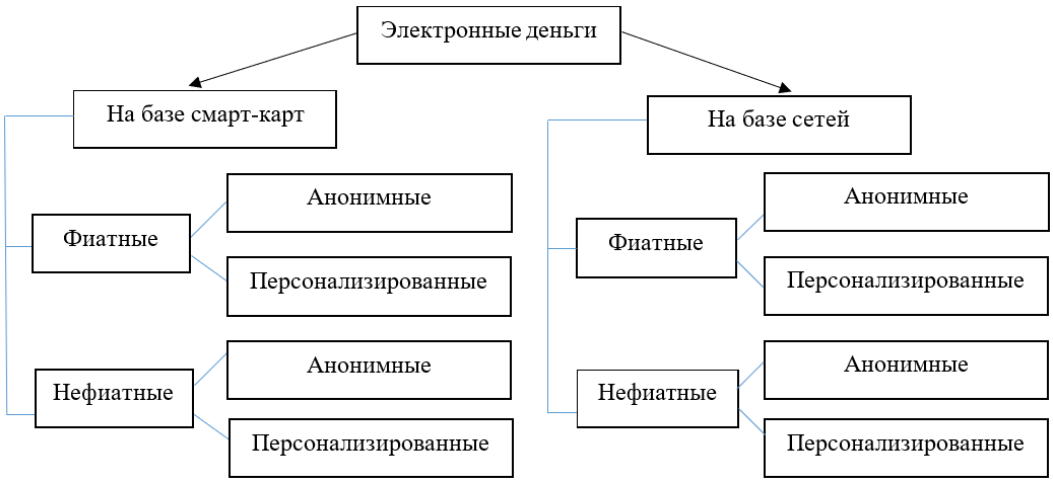

Рис.1. Классификация электронных денег
Fig.1. Classification of electronic money

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ИХ ОБСУЖДЕНИЕ

Выполнив сравнение обычных денежных знаков и цифровой наличности, можно сделать вывод, что обычная форма валюты проигрывает цифровой валюте. При использовании обычных денежных знаков отсутствует возможность провести идентификацию личности. Похищенные как материальный носитель, их будет почти невозможно отследить. При использовании персонализированных электронных систем, всегда можно будет узнать, кто произвел платеж. Наличные деньги, как предмет, является разносчиком инфекций, поскольку передается из рук в руки. Эпидемия COVID-19 показала, насколько опасно может быть использование таких носителей. Совершая же платежи по сети, или используя смарт карту, пользователь не контактирует с лишними предметами. Электронные деньги куда проще хранить, передавать на расстояния, а их номинал никак не связан с массой и габаритами хранителя.

Недостатки цифровой наличности во многом связанны с неприятием информационных технологий в мире. Статистика показывает, что в России значительная часть населения не пользуется банковской картой вообще, или же использует ее только для снятия наличных денег. Большинство людей старшего поколения имеют трудности с использованием компьютера, а соответственно, и с использованием цифровой наличности.

Исследование безопасности систем цифровой наличности заключается в выделении уязвимостей отдельных типов такой наличности.

Рассматривая электронные деньги на базе сетей, выделяются фиатные деньги (системы PayPal, M-Pesa), и нефиатные (системы WebMoney, Яндекс.Деньги, криптовалюты на базе Bitcoin). [9, 2] Для электронной наличности на базе сетей свойственны те уязвимости, которыми обладают все базы данных, расположенные в сети. Так, возможна кража данных, используемых для аутентификации – это логин и пароль для доступа к профилю, коды для восстановления профиля и т. д. Для предотвращения этой уязвимости можно использовать двухфакторную аутентификацию, включить уведомление о подтверждении операций, и т д. Но как правило, такие функции привязаны к одному устройству (чаще всего к телефону), и его похищение дает доступ злоумышленнику к кошельку. Имеют место быть и методы социальной инженерии, когда злоумышленник может получить доступ к данным, используя различные способы воздействия на хозяина кошелька [1].

Такие системы также подвержены хакерским атакам. К примеру, одна из последних уязвимостей системы PayPal была связанна с тем, как PayPal хранит токены CSRF и ID сессий в файле JavaScript, из-за чего они становились доступными для злоумышленников посредством XSSI-атак. Хотя для рандомизации имен при каждом запросе использовался обфускатор, все равно имелась возможность предсказать, где находятся токены и извлечь их.

Следует отдельно отметить уязвимости криптовалют, работающих на базе Bitcoin. Поскольку на сегодняшний день Bitcoin, а также работающие на его базе другие криптосистемы (Litecoin, Namecoin и др.) наиболее популярны, и внимание к таким системам более высокое. Bitcoin свойственны системные проблемы, к примеру взлом через бэкап кошелька. Восстановление старого кошелька с паролем восстанавливает текущий кошелек и текущий пароль. Существует Атака Сивиллы, что позволяет хакеру наполнить сеть подконтрольными ему узлами, и остальные пользователи смогут подключиться только к блокам, созданным для мошенничества [4].

Несмотря на анонимность системы, существует возможность проследить историю денежных транзакций. К тому же баланс кошелька находится в открытом доступе, и не каждый пользователь будет на это согласен [3].

Альтернативой электронной наличности на базе сетей будет использование смарт-карт. Это карта, содержащая микропроцессор и операционную систему, управляющую устройством и контролирующую доступ к объектам в его памяти. Кроме того, смарт-карты, как правило, обладают возможностью проводить криптографические вычисления. Не следует путать такое устройство с обычной банковской картой: банковские карты предоставляют доступ к банковскому счету, а на смарт-карте деньги хранятся в виде цифрового эквивалента. Это, в свою очередь,

позволяет проводить операции в режиме off-line. Примерами таких систем служат Visa Cash, Mondex, «Октопус» и другие.

Среди уязвимостей смарт карт, в первую очередь, следует выделить уязвимость криптоалгоритмов смарт-карт, так как они практически полностью доступны. Но, такие уязвимости быстро устраняют. Существует также вероятность дифференциального анализа питания. Оценка осциллограмм потребляемой смарт-картой электроэнергии в момент выполнения криптоалгоритма.

Следует отметить и тот факт, что смарт-карта – это физический носитель, который можно похитить. К примеру, можно получить доступ к электрическим цепям смарт-карты после химического снятия защитных слоев с кристалла. Это позволит провести анализ устройства смарт-карты и подключиться к ней с помощью микроэлектродов. Также, карта уязвима к необычным условиям окружающей среды, среди которых температура, магнитное воздействие и т.д.

В целом, по результатам исследования, делается вывод, что основную проблему перед внедрением электронной наличности играет не её уязвимость, а недоверие к таким системам со стороны общества и государства. Обращаясь к наиболее экономически развитым странам, можно отметить, что оборот наличных денег среди населения падает. Переход на электронную наличность также позволит снизить уровень преступности, и в особенности финансовых преступлений [6, с. 5-6]. В большинстве своем, мировая преступность всегда ведёт свои дела через наличные деньги. Конечно, имеет место использование криптовалют в мировой преступности, но её отследить проще, чем обычную наличность.

Для увеличения оборота цифровых денег, в первую очередь, следует бороться с недоверием к электронной наличности среди населения. Приобщение общества к цифровым технологиям, демонстрация преимуществ электронной наличности, значительно увеличит распространение цифровых денег.

ЗАКЛЮЧЕНИЕ

По результатам исследования, можно сделать вывод, что электронная наличность имеет больше преимуществ, чем недостатков, перед обычными денежными знаками.

Исходя из сравнений различных типов электронной наличности, нельзя сделать однозначный вывод, какой из систем следует отдать предпочтение. При выборе пользователь должен исходить из своих потребностей. Для обеспечения наибольшей безопасности своих средств, следует отдать предпочтение персонализированным фиатным системам, построенным на базе сетей, поскольку такие системы имеют наиболее совершенную систему подтверждения подлинности, надежную систему аутентификации пользователя, и обеспечение надежности курса валюты со стороны Центробанка.

При требовании высокого уровня анонимности следует обращаться к нефиатным анонимным системам криптовалют, особенно к системам, работающих на алгоритме круговой подписи (Bytecoin, Monero).

При требовании возможности работы off-line, предпочтение следует отдавать системам на смарт-картах.

Список литературы

1. Абдеева З.Р. Электронные новации платежных систем посредством банковских карт и электронных денег // Российское предпринимательство. – 2014. – № 24(270). – С. 109-114.
2. Ermakov N.S., Galkina E.A. Global approach to e-money protection and risk diversification // В сборнике: XXXIII International plekhanov readings. – 2020. – С. 19-25.
3. Какаев Д.В., Маслова М.А. Обзор вирусов удаленного доступа для мобильных устройств // Научный результат. Информационные технологии. – 2020. – Т. 5. – № 1. – С. 27-34.
4. Маслова М.А., Рыжая К.Ю. Интернет–мошенничество как угроза информационной безопасности личности // НБИ технологии. – 2019. – Т. 13. – № 2. – С. 25-28.
5. Минусы наличных денег [Электронный ресурс] – Режим доступа: https://benefit.by/page/show/articles/1651 (Дата обращения: 25.07.2020)

6. Миронкина А.Ю. Отказ от наличных денег: достоинства и недостатки // Синергия наук. – 2016. – № 5. − С. 54−60.
7. Строителева Е.В., Мигачев И.Б. Электронные деньги: виды, сущность и перспективы развития // Алтайский институт финансового управления, г. Барнаул, Россия – 2014.
8. Цифровые наличные [Электронный ресурс] – Режим доступа: http://kunegin.com/ref6/ecom/43.htm (Дата обращения: 24.07.2020)
9. Частные электронные деньги [Электронный ресурс] – Режим доступа: https://www.fd.ru/articles/62433-chastnye-elektronnye-dengi (Дата обращения: 25.07.2020)
10. Электронные денежные системы [Электронный ресурс] – Режим доступа: https://sites.google.com/site/elektronnyedeneznyesistemy/ (Дата обращения: 25.07.2020)

References

1. Abdeeva Z.R. Electronic innovations of payment systems via Bank cards and electronic money// Russian entrepreneurship. – 2014. – No. 24(270). – Pp. 109-114.
2. Ermakov N.S., Galkina E.A. Global approach to e-money protection and risk diversification // In: XXXIII International plekhanov readings. – 2020. – Pp. 19-25.
3. Kakaev D.V., Maslova M.A. Review of remote access viruses for mobile devices. // Research result. Information technology. – 2020. – Vol. 5. – No. 1. – Pp. 27-34.
4. Maslova M.A., Ryzhaya K.Yu. Internet-fraud as a threat to personal information security // NBI technologies. – 2019. – Vol. 13. – No. 2. – Pp. 25-28.
5. Cons of cash [Electronic resource] – access Mode: https://benefit.by/page/show/articles/1651 (accessed: 25.07.2020)
6. Mironkina A. Yu. Refusal of cash: advantages and disadvantages // Synergy of Sciences. – 2016. – No. 5. – P. 54-60.
7. Stroiteleva E. V., Migachev I. B. Electronic money: types, essence and prospects of development // Altai Institute of financial management, Barnaul, Russia-2014.
8. Digital cash [Electronic resource] – access Mode: http://kunegin.com/ref6/ecom/43.htm (accessed: 24.07.2020)
9. Private electronic money [Electronic resource] – access Mode: https://www.fd.ru/articles/62433-chastnye-elektronnye-dengi (accessed: 25.07.2020)
10. Electronic money systems [Electronic resource] – access Mode: https://sites.google.com/site/elektronnyedeneznyesistemy/ (accessed 25.07.2020)

Шевцов Максим, студент 4 курса кафедры «Информационная безопасность» Института радиоэлектроники и информационной безопасности
Маслова Мария Александровна, аспирант, старший преподаватель кафедры «Информационная безопасность» Института радиоэлектроники и информационной безопасности

Shevtsov Maxim, 4th year student of the Department «Information security»», Institute of Radioelectronics and Information security
Maslova Maria Alexandrovna, post-graduate student, senior lecturer of the Department «Information security», Institute of Radioelectronics and Information security

УДК 004.056.53 **DOI: 10.18413/2518-1092-2020-5-3-0-3**

Девицына С.Н.
Гоголь А.С.

РАЗРАБОТКА МЕТОДА СОЗДАНИЯ КАПЧИ, УСТОЙЧИВОЙ К АВТОМАТИЧЕСКОМУ РАСПОЗНАВАНИЮ И УГАДЫВАНИЮ

Севастопольский государственный университет, ул. Университетская, д. 33, г. Севастополь, 299053, Россия

e-mail: sndevitsyna@sevsu.ru, andrewgogol777@gmail.com

Аннотация
Актуальность рассматриваемой в статье проблемы обусловлена тем, что растет количество веб-ресурсов различных государственных организаций и коммерческих компаний в сети Интернет, а одной из причин утечки данных может являться массовый сбор информации. Полученные при сборе сведения могут стать инструментом в умелых руках злоумышленника. Злоумышленники могут спокойно создавать и выгружать в сеть вредоносное программное обеспечение с функциями сбора информации, собранная информация может использоваться для осуществления атак с мощью методов социальной инженерии. Самыми подходящими методами для таких атак являются фишинг и претекстинг. В статье предлагается обзор проблемы незаконного массового сбора информации и использование её злоумышленниками. Проанализированы возможные методы противодействия массовому сбору информации, рассмотрены варианты создания капч, и их недостатки – возможность распознавания и угадывания злоумышленником, или ботом. В результате предложен улучшенный метод, который решает данную проблему. В работе описаны основные функции работы программы, а также возможные вариации использования генерации капчи. Для защиты от распознавания капчи обученным ботом, предложено вводить в изображение смысловую нагрузку. В результате разработан и представлен метод создания капчи, устойчивой к автоматическому распознаванию текста.
Ключевые слова: информационные технологии; информационная безопасность; капча; авторизация; сбор информации; распознавание образов.

UDC 004.056.53

Devitsyna S.N
Gogol A.S.

DEVELOPING A METHOD FOR CREATING A RESISTANT TO AUTOMATIC RECOGNITION AND GUESSING CAPTCHA

Sevastopol state University, 33 Universitetskaya St., Sevastopol, 299053, Russia

e-mail: sndevitsyna@sevsu.ru, andrewgogol777@gmail.com

Abstract
The relevance of the problem considered in the article is due to the growing number of web resources of various government organizations and commercial companies on the Internet, and one of the reasons for data leakage may be mass collection of information. The information obtained during the collection can become a tool in the capable hands of an attacker. Attackers can easily create and upload malicious software with information collection functions to the network, and the collected information can be used to carry out attacks with the power of social engineering methods. The most suitable methods for such attacks are phishing and pretexting. The article provides an overview of the problem of illegal mass collection of information and its use by hackers. Possible methods of countering mass data collection are analyzed, options for creating captchas are considered, and their disadvantages are the possibility of recognition and guessing by an attacker or bot. As a result, an improved method is proposed that solves this problem. This paper describes the main functions of the program, as well as possible variations in the use of captcha generation. To protect against captcha recognition by a trained bot, it is suggested to enter a semantic load into the image. As a result, we developed and presented a method for creating a captcha that is resistant to automatic text recognition.

Keywords: information technology; information security; CAPTCHA; authorization; information collection; image recognition.

ВВЕДЕНИЕ

Применение методик социальной инженерии приводит к тому, что сотрудник компании разглашает сведения, которые несут определенную ценность для организации, в которой он работает. Данные методики могут использоваться также и для осуществления атак на рядовых пользователей, например, для сбора сведений о банковском счете, либо банковской карте.

Для защиты веб-ресурсов от массового сбора информации пользователей, которая потом может использоваться злоумышленниками, администратор и разработчики сайта могут использовать защитное программное обеспечение. Некоторые из применяемых средств имеют недостатки, которые были учтены и удалены при разработке программы для защиты сайта от ботов.

Действенным инструментом злоумышленников являются сети из зараженных вирусами компьютеров. Данные сети называют ботнетами [Kaspersky, 2020], они используют чужие вычислительные мощности, а также занимаются саморасширением, и запрограммированы на какие-либо повторяющиеся действия. В эти повторяющиеся действия может входить и сбор информации. Для человека это – очень длительный процесс, в то время как бот справится с ним намного быстрее. Предлагаемый программный продукт будет включать в себя и предупреждения для людей, чьи компьютеры оказались частью сети злоумышленника.

Целью исследования является улучшение существующих методов защиты сайтов от массового сбора информации. Для достижения поставленной цели решены следующие задачи:

- проанализированы существующие меры защиты сайтов от массового сбора информации;
- разработан алгоритм действий для защиты сайтов от массового сбора информации.

ОСНОВНАЯ ЧАСТЬ

С развитием информационных технологий Тест Тьюринга [Turing test, 2020] нашел свое применение в повседневной работе сайтов и защите их от сбора информации. Для защиты от массового сбора информации часто используют тесты, такие, как капча.

Капча – тест, который является модификацией теста Тьюринга и служит для распознавания и отсеивания ботов с веб-ресурсов [Habr, 2009; reCAPTCHA 2020; Habr, 2011].

Различают следующие виды тестов:

- интерактивные тесты;
- иллюстративные тексты;
- тесты на логику;
- тесты со смысловой нагрузкой;
- текстово-цифровые тесты.

Все виды капч имеют свои особенности [CAPTCHA, 2020; reCAPTCHA 2020; Rucaptcha. 2020]. Например, чтобы пройти интерактивный тест, необходимо взаимодействовать с интерфейсом сайта, и пользователя могут попросить передвинуть ползунок в необходимое положение. Чтобы пройти капчу со смысловой нагрузкой, пользователя могут попросить решить легкую загадку, либо проверить его на внимательность. В случае теста на логику можно попросить пользователя решить математический пример: сложить 1 и 2. Каждая такая программа должна использоваться администратором на основании каких-либо признаков, либо может работать в автоматическом режиме.

Самыми слабыми капчами являются текстово-цифровые и логические [Пудовикова П.Д., Титов С.С., 2016]. Логические можно перебрать, а текстово-цифровые можно распознать. При разработке метода создания капчи необходимо не только учесть недостатки существующих видов капчи, но и то, что существуют группы лиц, которые работают над распознаванием капч. Таким образом, метод должен позволить отсеивать определенную часть таких злоумышленников.

Злоумышленники могут использовать базы данных, которые содержат в себе миллионы ответов на разные капчи. Чтобы избавиться от этой проблемы, необходимо улучшить количество вариаций при генерации изображения капчи. Признаками взлома могут являться: необычное поведение пользователя, повторяющиеся безрезультативные действия, использование и переходы по скрытым ссылкам, либо странные движения мышью.

Надежный алгоритм теста должен обладать такими свойствами как:

- устойчивость к распознаванию;
- защита от перебора;
- устойчивость к угадыванию.

При выборе вида капчи рассматривались недостатки существующих методов. Например, на рис. 1 представлена слабая капча с фиксированным и неискаженным шрифтом. Такой капче свойственны легкость отделения текста с помощью цветового ключа и легкость отделения символов друг от друга.

На рисунке видно отделение символов, которые темнее определенного уровня, таким образом работает автоматическое распознавание текста. Весь остальной фон заполняется белым цветом.

Рис. 1. Пример разбора слабой капчи
Fig. 1. Example of parsing a weak captcha

На рис. 2 представлен пример сильной капчи – reCAPTCHA от компании Google [reCAPTCHA 2020]. Для ее генерации компания Google использует слова, которые не смогли распознать их боты. Для большей надежности используется проверочное слово, данное слово намеренно искажается. В этом случае рекомендуется дублировать текст, либо использовать горизонтальное и вертикальное искажение.

В капче компании Google слова берутся из старых учебников, которые оцифровали для перевода в электронный формат и хранят на серверах компании. Для большей точности предлагается пройти тест с одним и тем же словом тысячам пользователей.

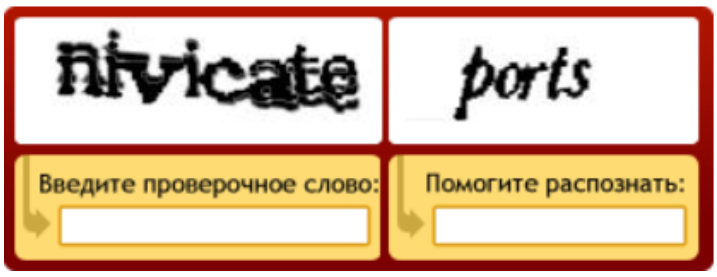

Рис. 2. Пример сильной reCAPTCHA от компании Google
Fig. 2. Example of a strong reCAPTCHA from Google

Проанализировав сильные и слабые стороны разных видов капчи, принято решение предложить альтернативный вариант, позволяющий защитить капчу от автоматического распознавания и угадывания. Для разработки приложения были выбран язык Python [Sololearn Python, 2020].

На рис. 3 представлена структурная схема алгоритма работы программы, которая включает в себя следующие функции:

- функция создания матрицы с данными для демонстрации работы с пользователями;
- функция генерации случайной строки из букв и цифр;
- функция нанесения текста на изображение;
- функция цветовой инверсии;
- функция проверки пользователя.

Рис. 3. Структурная схема алгоритма программы
Fig. 3. Block diagram of the program algorithm

Рассмотрим три функции, которые определяют устойчивость разработанного метода. Это – функции генерации случайной строки, функция нанесения текста на изображения, а также функция цветовой инверсии. Все эти функции связаны принципами функционального программирования и создают устойчивую к распознаванию капчу. В каждую из последующих функций заходит значение, которое возвращает предыдущая функция.

Основными инструментами создания устойчивой к автоматическому распознаванию капчи являются: функция генерации капчи, нанесения капчи на изображение из базы данных изображений и функция цветовой инверсии.

На рис. 4 приведен сгенерированный случайный текст, состоящий из букв кириллицы и цифр. Использование кириллических букв позволит частично отсеять сегмент иностранных злоумышленников, выполняющих распознавание капч.

Функция работает с заранее прописанной строкой, в которой имеются цифры от 0 до 9 и буквы кириллицы. Далее, с помощью библиотеки random и определенного метода, выбирается случайное количество символов в пределах от 7 до 9 из заранее определенной строки. Данная функция сохраняет результат своей работы в список, первый и единственный элемент которого – это выбранные символы.

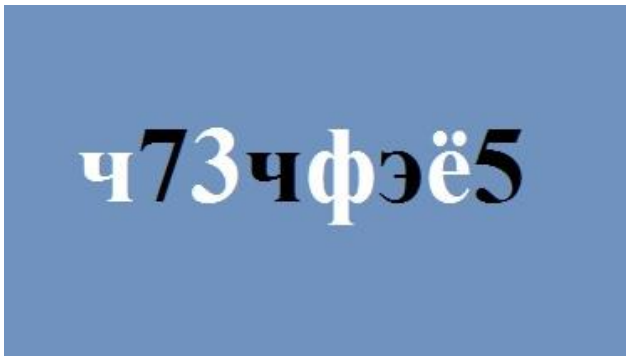

Рис. 4. Сгенерированный текст
Fig. 4. Generated text

На рис.4 видно, что текст уже перекрашен в черно-белый цвет, но данное преобразование должна выполнять функция нанесения текста на изображение с помощью использования библиотеки PIL. Работа с данной библиотекой возможна при использовании среды разработки PyCharm и установленного пакета библиотек Anaconda.

PyCharm – это интегрированная среда разработки (IDE), используемая в компьютерном программировании, особенно часто для языка Python. Она разработана чешской компанией JetBrains. PyCharm включает в себя анализ кода, графический отладчик, встроенный тестер модулей, интеграцию с системами контроля версий (VCSes), и поддерживает веб-разработку с Django, а также DataScience с Anaconda [Anaconda, 2020; Pycharm, 2020].

Anaconda – дистрибутив языков программирования Python и R, включет набор популярных бесплатных библиотек, объединенных проблемами науки о данных и машинного обучения. Основная цель – предоставить тематическим модулям единый согласованный набор наиболее востребованных соответствующим кругом пользователей для разрешения возникающих зависимостей и конфликтов, которые неизбежны при одной установке [Sololearn Python, 2020.].

На рис. 5 представлен пример работы функции нанесения символов на изображение с помощью методов DrawText. При нанесении создаются два списка разных цветов с пробелами, что позволяет нанести символы черно-белого цвета в том порядке, в котором они были сгенерированы.

Рис. 5. Нанесение сгенерированного текста на выбранное изображение
Fig. 5. Applying the generated text to the selected image

На рис. 6 представлен результат работы функции инверсии изображения, которое получено из функции нанесения текста на изображение. Именно это изображение будет представлено боту, либо человеку. Пользователя попросят ввести символы, например, белого цвета, расположенные в верхней части изображения. Можно предложить выбрать символы черного цвета, либо комбинировать области изменения цвета, либо просить его ввести символы того или иного цвета из верхней части изображения. Комбинации могут быть различными, главное – наличие

смысловой нагрузки и обеспечение выбора заданных типов символов для прохождения аутентификации.

Рис. 6. Пример готовой капчи с инверсией пикселей
Fig.6. Example of a ready-made captcha with pixel inversion

Помимо всего, необходимо предупреждать пользователя, что его компьютер может являться частью ботнета, что, возможно, поможет исключить один бот из сети злоумышленника. В программе учитывался данный фактор, так как перед тестом мог находиться пользователь, чей компьютер нес в себе вредоносное программное обеспечение, а не автономный бот, который использует ресурсы злоумышленника, либо сервисы для сканирования сайтов.

В результате работы была получена капча, устойчивая к автоматическому распознаванию текста. Так как не исключается возможность распознавания данной капчи обученным ботом, в ней присутствует смысловая нагрузка, а именно – просьба ввести определенные символы с той или иной области изображения.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

В результате исследования был выявлен ряд недостатков во всех видах существующих тестов. Для создания устойчивой капчи предложено комбинировать методы из каждого типа капч. При создании устойчивого к автоматическому распознаванию и угадыванию метода была использована комбинация двух видов капч: текстово-цифровая капча и капча со смысловой нагрузкой. Смысловая нагрузка является страховкой метода, которая защищает его от автоматического распознавания текста. Также были учтены физиологические особенности человека: так как не каждый человек может различать цвета, предложено использовать простую черно-белую гамму. Также плюсы данной капчи в том, что можно выбирать тематику изображения, что позволит использовать ее на сайтах различных государственных организаций и компаний. Количество вводов и время ввода может выставлять сам администратор сайта. Данный программный продукт, написанный на языке программирования Python, может использоваться большим количеством веб-ресурсов, так как основным их языком является язык Python.

ЗАКЛЮЧЕНИЕ

Сегодня у злоумышленников имеется огромное количество ресурсов в виде программ-скрапперов в составе ботнета, автономных ботов и общедоступных интернет-утилит. Преступники могут собирать информацию не только сами, но и с помощью чужих ресурсов, что увеличивает масштабы сканирования и сбора информации. Следовательно, это влечет за собой определенные угрозы для рядовых пользователей и сотрудников организаций.

В статье показан улучшенный метод создания капчи, предложенный Гоголем А.С. в рамках выпускной квалификационной работы бакалавра, также представлены функции и алгоритм программы для защиты сайтов от массового сбора информации. К достоинствам улучшенного алгоритма, написанного на языке Python с использованием среды разработки PyCharm, можно отнести:

- устойчивость к распознаванию текста;
- наличие смысловой нагрузки;
- простая цветовая гамма;
- наличие предупреждения для пользователя.

Данную капчу можно использовать как при работе пользователя на сайте, так и для процедуры авторизации.

Список литературы

1. Anaconda, 2020. URL: https://www.anaconda.com (дата обращения 05.05.2020).
2. CAPTCHA: Telling Humans and Computers Apart Automatically. URL: http://captcha.net (дата обращения 03.05.2020).
3. Habr, 2011. Как работает reCAPTCHA? URL: https://habr.com/ru/post/121010 (дата обращения 03.05.2020).
4. Habr, 2009. Тест Тьюринга. URL: https://habr.com/ru/post/69758 (дата обращения 01.05.2020).
5. Kaspersky, 2020. Что такое ботнет? URL: https://www.kaspersky.ru/resource-center/threats/botnet-attacks (дата обращения 01.05.2020).
6. Pycharm, 2020. Jetbrains Developer Tool. URL:https://www.jetbrains.com/pycharm (дата обращения 03.05.2020).
7. reCAPTCHA, 2020. The new way to stop bots. URL: https://www.google.com/recaptcha/intro/v3.html (дата обращения 03.05.2020).
8. Rucaptcha. 2020. URL: https://rucaptcha.com/software/category/skripti-i-biblioteki (дата обращения 03.05.2020).
9. Sololearn Python, 2020. URL: https://www.sololearn.com/Play/Python (дата обращения 03.05.2020).
10. Turing test, 2020. From Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Turing_test (дата обращения 03.05.2020).
11. Пудовикова, П.Д., Титов, С.С., 2016. Метод реализации captcha на основе подбора области изображения. URL: https://elibrary.ru/item.asp?id=28335822 (дата обращения 07.05.2020).

References

1. Anaconda, 2020. URL: https://www.anaconda.com/ (date of circulation: 05.05.2020).
2. CAPTCHA, 2020. Telling Humans and Computers Apart Automatically. URL: http://captcha.net (date of circulation: 03.05.2020).
3. Habr, 2011. How it works reCAPTCHA? URL: https://habr.com/ru/post/121010 (date of circulation: 03.05.2020).
4. Habr, 2009. Turing test. URL: https://habr.com/ru/post/69758 (date of circulation: 01.05.2020).
5. Kaspersky, 2020. What is a botnet? URL: https://www.kaspersky.ru/resource-center/threats/botnet-attacks (date of circulation: 01.05.2020).
6. Pycharm, 2020. Jetbrains Developer Tool. URL: https://www.jetbrains.com/pycharm (date of circulation: 03.05.2020).
7. reCAPTCHA, 2020. The new way to stop bots. URL: https://www.google.com/recaptcha/intro/v3.html (date of circulation: 03.05.2020).
8. Rucaptcha, 2020. URL: https://rucaptcha.com/software/category/skripti-i-biblioteki (date of circulation: 03.05.2020).
9. Sololearn Python, 2020. URL: https://www.sololearn.com/Play/Python (date of circulation: 03.05.2020).
10. Turing test, 2020. From Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Turing_test (date of circulation: 03.05.2020).
11. Pudovikova P.D., Titov S.S., 2016. Method of implementation captcha based selection of the images URL: https://elibrary.ru/item.asp?id=28335822 (date of circulation: 07.05.2020).

Девицына Светлана Николаевна, кандидат технических наук, доцент, доцент кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности
Гоголь Андрей Сергеевич, студент 4 курса кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности

Devitsyna Svetlana Nikolaevna, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department Information security, Institute of Radioelectronics and Information security
Gogol Andrey Sergeevich, 4th year student of the Department Information security, Institute of Radioelectronics and Information security

АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ
INFORMATION SYSTEM AND TECHNOLOGIES

УДК 004.048 **DOI: 10.18413/2518-1092-2020-5-3-0-4**

Кононов В.М.[1]
Асадуллаев Р.Г.[2]
Щетинина Е.С.[2]
Афонин А.Н.[2]

АЛГОРИТМ ПРЕДВАРИТЕЛЬНОЙ ОБРАБОТКИ НЕЙРОФИЗИОЛОГИЧЕСКИХ ДАННЫХ

[1)] ООО «ЦентрПрограммСистем», ул. Восточная, д.71, г. Белгород, 308019, Россия
[2)] Белгородский государственный национальный исследовательский университет, ул. Победы, д. 85, г. Белгород, 308015, Россия

e-mail: kononov@1cps.ru, asadullaev@bsu.edu.ru, 1198621@bsu.edu.ru, afonin@bsu.edu.ru

Аннотация
Статья посвящена разработке алгоритма предварительной обработки нейрофизиологических данных, полученных при помощи fNIRS (функциональной ближней инфракрасной спектроскопии). Данный алгоритм может применяться при сборе и систематизации набора данных для обучения и тестирования нейронных сетей глубокого обучения с целью выявления нейрофизиологических паттернов движений человек, а также для статистического анализа данных, полученных экспериментальным путем. Отличительной особенностью разработанного алгоритма является гибкость настройки алгоритма, а также возможность адаптации под требования к обработке, предъявляемые в зависимости от специфики решаемой задачи. Полученный алгоритм позволил сформировать набор данных, на котором обучалась нейронная сеть для распознавания паттернов активности кисти руки.
Ключевые слова: машинное обучение; fNIRS; нейронные сети; нейрофизиологические данные.

UDC 004.048

Kononov V.M.[1]
Asadullaev R.G.[2]
Shchetinina E.S.[2]
Afonin A.N.[2]

PRE-PROCESSING NEUROPHYSIOLOGICAL DATA ALGORITHM

[1)] LLC «CenterProgramSystem», 71 Vostochnaya st., Belgorod, 308019, Russia
[2)] Belgorod State National Research University, 85 Pobedy St., Belgorod, 308015, Russia

e-mail: kononov@1cps.ru, asadullaev@bsu.edu.ru, 1198621@bsu.edu.ru, afonin@bsu.edu.ru

Abstract
The article is devoted to the development of an algorithm for pre-processing of neurophysiological data obtained using fNIRS (functional near- infrared spectroscopy). The developed algorithm can be used for the picking and systematization of a data set for training and testing deep learning neural networks to identify neurophysiological patterns of human movements. Also, the algorithm can be used for statistical analysis of data obtained experimentally. A distinctive singularity of the developed algorithm is the flexibility of constructing and the adapt ability to the processing requirements presented, depending on the

specifics of the problem. The developed algorithm allows to form a data set for neural network training and to recognize patterns of activity of the human wrist.
Keywords: machine learning; fNIRS; neural networks; neurophysiological data.

ВВЕДЕНИЕ

В настоящее время все большую популярность среди исследователей для анализа активности головного мозга набирает метод ближней инфракрасной спектроскопии(fNIRS) [4,8]. Эти данные используются исследователями для создания интерфейса мозг-компьютер, а также для обучения интеллектуальных систем, в том числе сетей глубокого обучения [1].

Актуальность данной работы заключается в расширении имеющихся знаний и подходов обработки данных fNIRS, заключающихся в разработке алгоритма, который может быть применен для решения прикладных задач формирования наборов данных, а также в возможности адаптации данного алгоритма под различные типы и размеры регистрируемых данных fNIRS [9].

ОСНОВНАЯ ЧАСТЬ

На выход разрабатываемого алгоритма предварительной обработки нейрофизиологических данных подаются регистрируемые сигналы активности головного мозга при помощи fNIRS. Экспериментальные данные получены в лаборатории НИУ «БелГУ». Возрастная группа респондентов – от 18 до 45 лет.

Разработан план эксперимента. Эксперимент состоял из повторения определенного цикла действий испытуемым в звукоизолированной аудитории без проникновения прямых солнечных лучей. Это обеспечило лучшую регистрацию данных оптического томографа и концентрацию респондентов на эксперименте.

Эксперимент проводился по следующему плану [5]:

– Начало эксперимента;

– Подготовка к началу выполнения команды участником после включения записи сигналов активности мозга – 10 секунд;

– Выполнить сжатие – 10 секунд;

– Выполнить разжатие – 10 секунд;

– Повторение данного цикла сжатия и разжатия 10 раз;

– Окончание эксперимента.

Во время эксперимента данные активности мозга регистрируются томографом в автоматическом режиме в файлы с расширением .wl1 и .wl2. Файлы NIRS-date_number.wl1 содержат записи 64 каналов, фиксирующие изменения оксигемоглобина в сосудах головного мозга во время проведения эксперимента. Файлы NIRS-date_number.wl2, NIRS-2020-04-30_006.wl2 содержат записи 64 каналов дезоксигемоглобина.

Так как, данные записываются без какой-либо обработки, появляется задача разработки алгоритма предварительной обработки исходных «сырых» экспериментальных данных. Под предварительной обработкой подразумеваются удаление шумов, выделение полезного сигнала, добавление меток и т.д.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ИХ ОБСУЖДЕНИЕ

Для решения поставленной задачи был написан ряд функций при помощи инструментов языка программирования Python и библиотек «numpy» и «tensorflow». Алгоритм предварительной обработки нейрофизиологических данных, полученных в ходе регистрации активности головного мозга при помощи fNIRS представлен на рисунке 1.

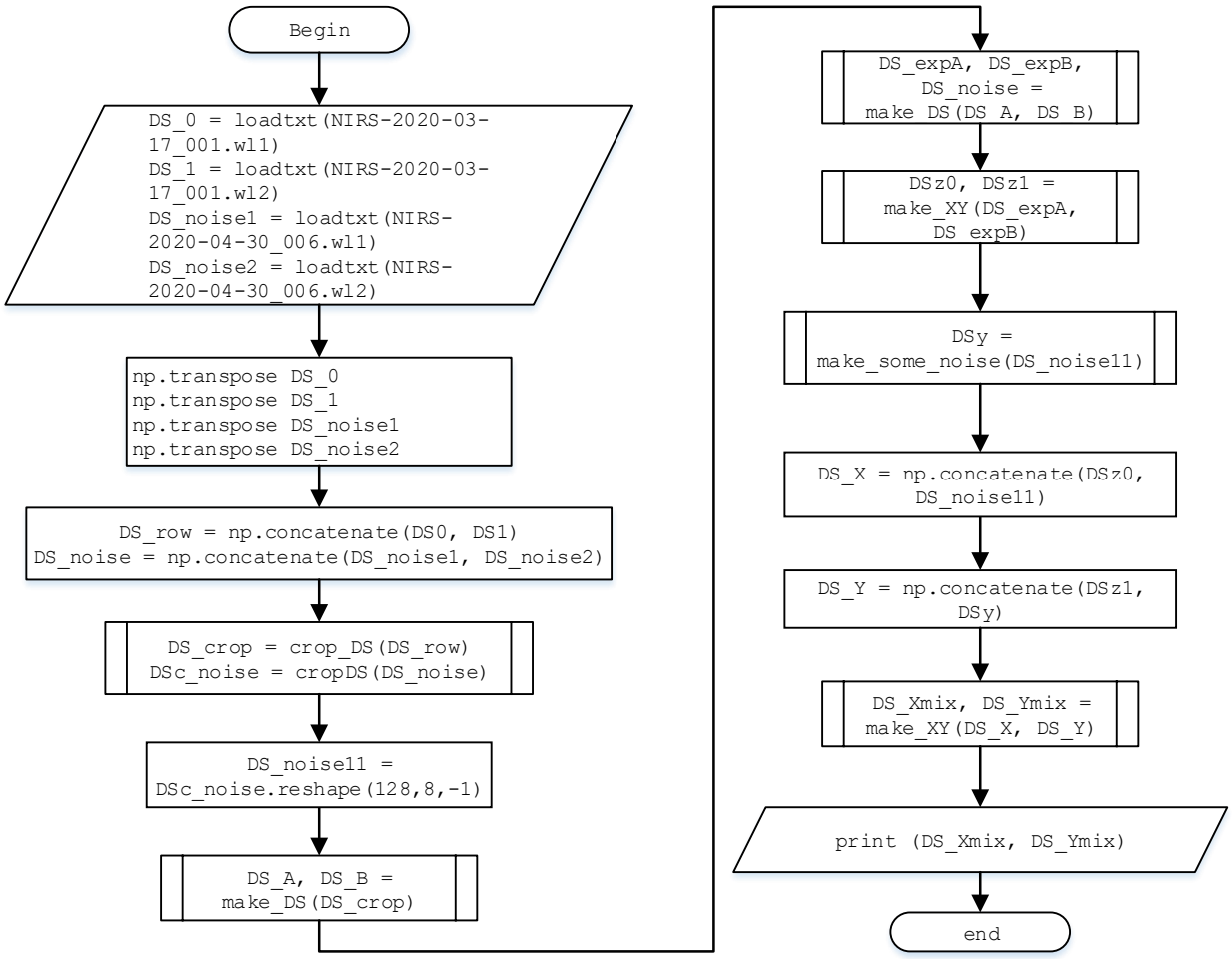

Рис. 1. Блок-схема алгоритма предварительной обработки нейрофизиологических данных
Fig. 1. Block diagram of the neurophysiological data preprocessing algorithm

Данная блок-схема состоит из следующих основных подпрограмм:

– удаление данных, не содержащих полезный сигнал;

– разделение данных всего эксперимента на команды составляющие, соответствующие командам «сжатие» и «разжатие»;

– выделение полезного сигнала, соответствующего выполнению одной команды, на интервалы заданного размера с перекрытием;

– формирование набора данных «шум»;

– перемешивание команд в наборе данных.

Изначальные данные хранятся в файлах NIRS-date_number.wl1 и NIRS- date_number.wl2 [3]. Каждый файл представлен в формате матрицы с размером CountFrame x 64, где 64 – количество каналов, а CountFrame – количество регистрируемых фреймов по каждому каналу (7,8Frame=1c.). Файлы загружаются и присваиваются в переменные DS_0, DS_1. Массивы DS_0 и DS_1 необходимо транспонировать, чтобы объединить данные динамики оксигемоглобина и дезоксигемоглобина в общий массив. В результате соединения формируется единый массив DS_row («сырой») размером 128 x CountFrame. Аналогичную процедуру проходят файлы NIRS-date_number.wl1 и NIRS-date_number.wl2, содержащие нецелевые команды для формирования единого массива DS_noise («шум»). Далее происходит удаление данных при помощи функции «crop_DS» (рисунок 2). Удаление происходит исходя из длинны входного массива «l», при этом отбрасываются данные, не содержащие полезной информации, а именно первые 10 секунд концентрации респондента на проведении эксперимента, а также шум, снятый после окончания

эксперимента, зафиксированный томографом. На обработку функции передаются массивы DS_row и DS_noise «crop_DS».

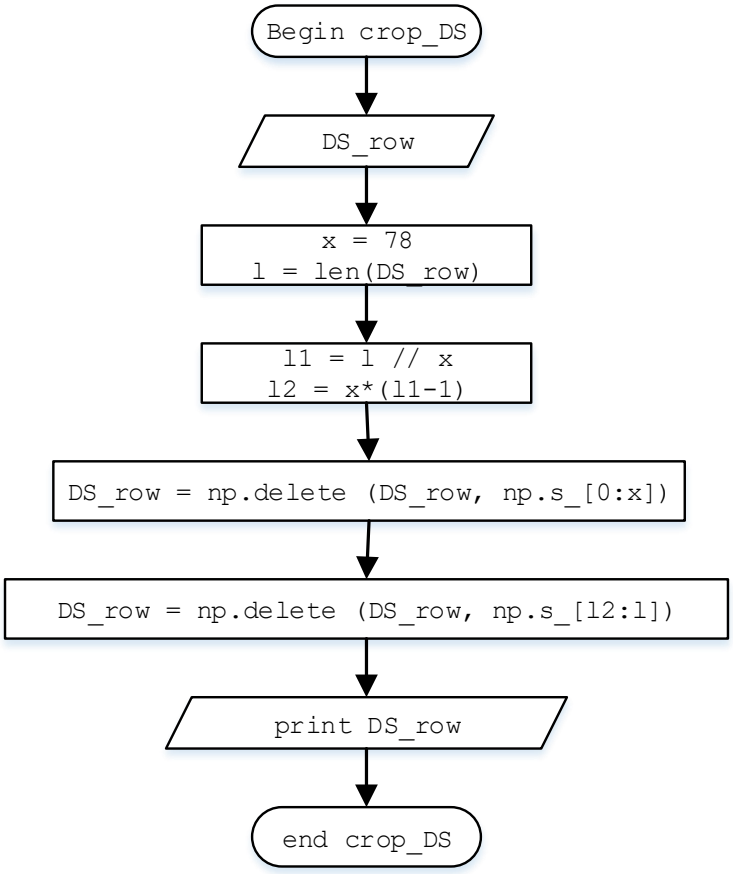

Рис. 2. Блок-схема функции «crop_DS»
Fig. 2. Block diagram of crop_DS function

После удаления происходит трансформирование выходного массива DSc_noise из двухмерного в трехмерный с размером 128x8xCountN, где 128 – количество каналов, 8 – количество фреймов за секунду шума, CountN – количество команд «шума», получаем массив DS_noise11.

Далее формируется массив DS_crop, который подается на функцию «make_DS». Функция «make_DS» формирует из одного потока «сырых» обрезанных данных два массива с набором команд («сжатие» кисти и «разжатие» кисти), которые были записаны последовательно с частотой 10 повторений по 10 секунд (рисунок 3) и представляет собой вложенный цикл с постусловием. В результате работы функции «make_DS» формируются массивы DS_A, содержащий команды «сжатие», и DS_B, содержащий команды «разжатие», что реализуется при помощи перезаписи каждых чётных 10 секунд в массив DS_A, и каждых нечётных 10 секунд в массив DS_B.

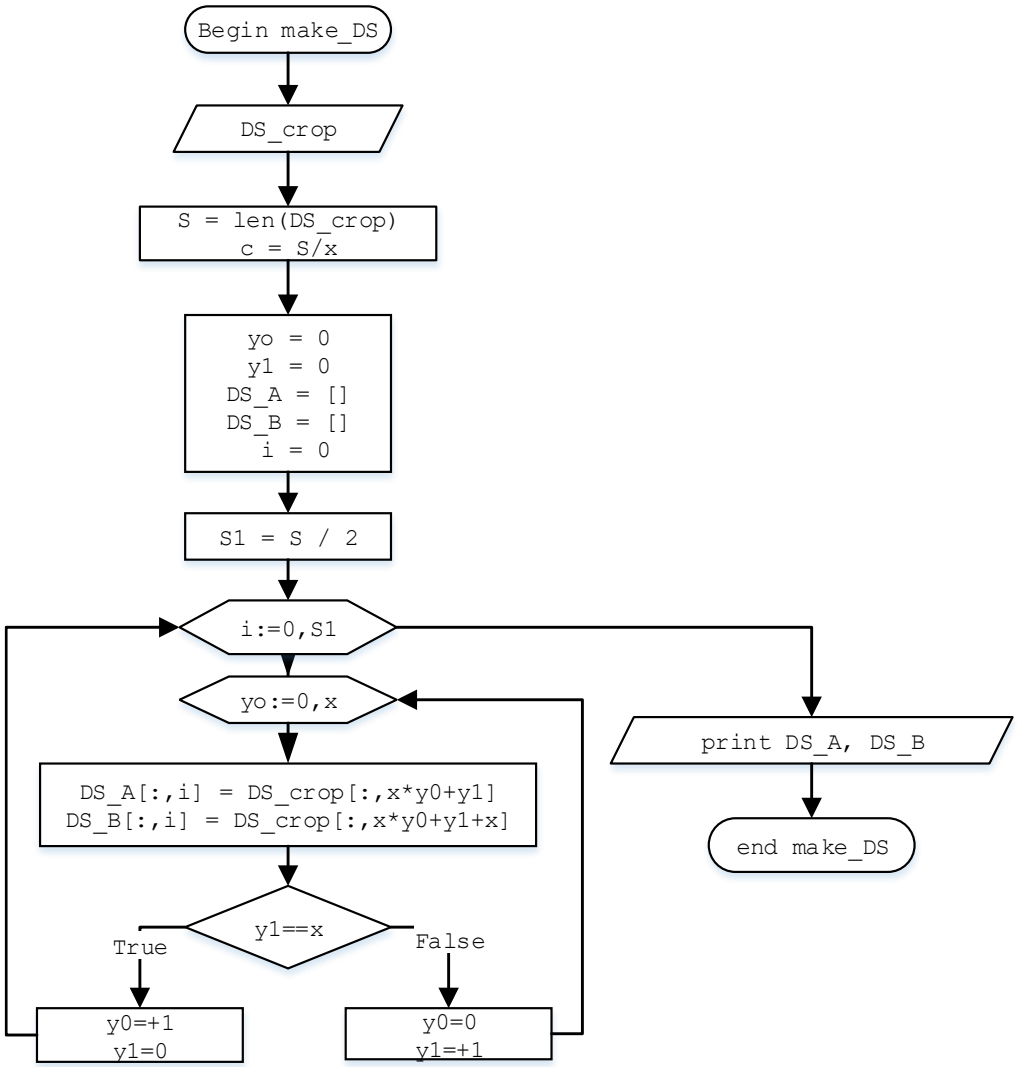

Рис. 3. Блок-схема функции «make_DS»
Fig. 3. Block diagram of make_DS function

Не все оставшиеся в массивах данные являются действительно полезной информацией. Из 10 секунд полезным является первоначальный всплеск сигнала за первые 4 секунды совершения команды «сжать кисть»/ «разжать кисть».

В связи с ограниченным количеством полезной информации, необходимо искусственно расширить имеющиеся данные массивов DS_A и DS_B, а также убрать из массивов данные, не содержащие целевых команд. Для решения данной задачи была разработана функция «exp_DS». Блок-схема функции «exp_DS» представлена на рисунке 4.

В зависимости от длин массивов DS_A, DS_B, формируются массивы DS_expA, DS_expB, в которые перезаписываются данные длинной 8 фреймов с шагом 4, то есть из каждых 10 секунд или 78 фреймов мы получаем 4 секунды или 32 фрейма полезного сигнала.

После прохождения цикла расширения полезного сигнала полученные массивы DS_expA и DS_expB транспонируются из двухмерных в трехмерные каждый с размером 128x8xCountC, где 128 – количество каналов, 8 – количество фреймов каждой команды, CountC – количество целевых команд.

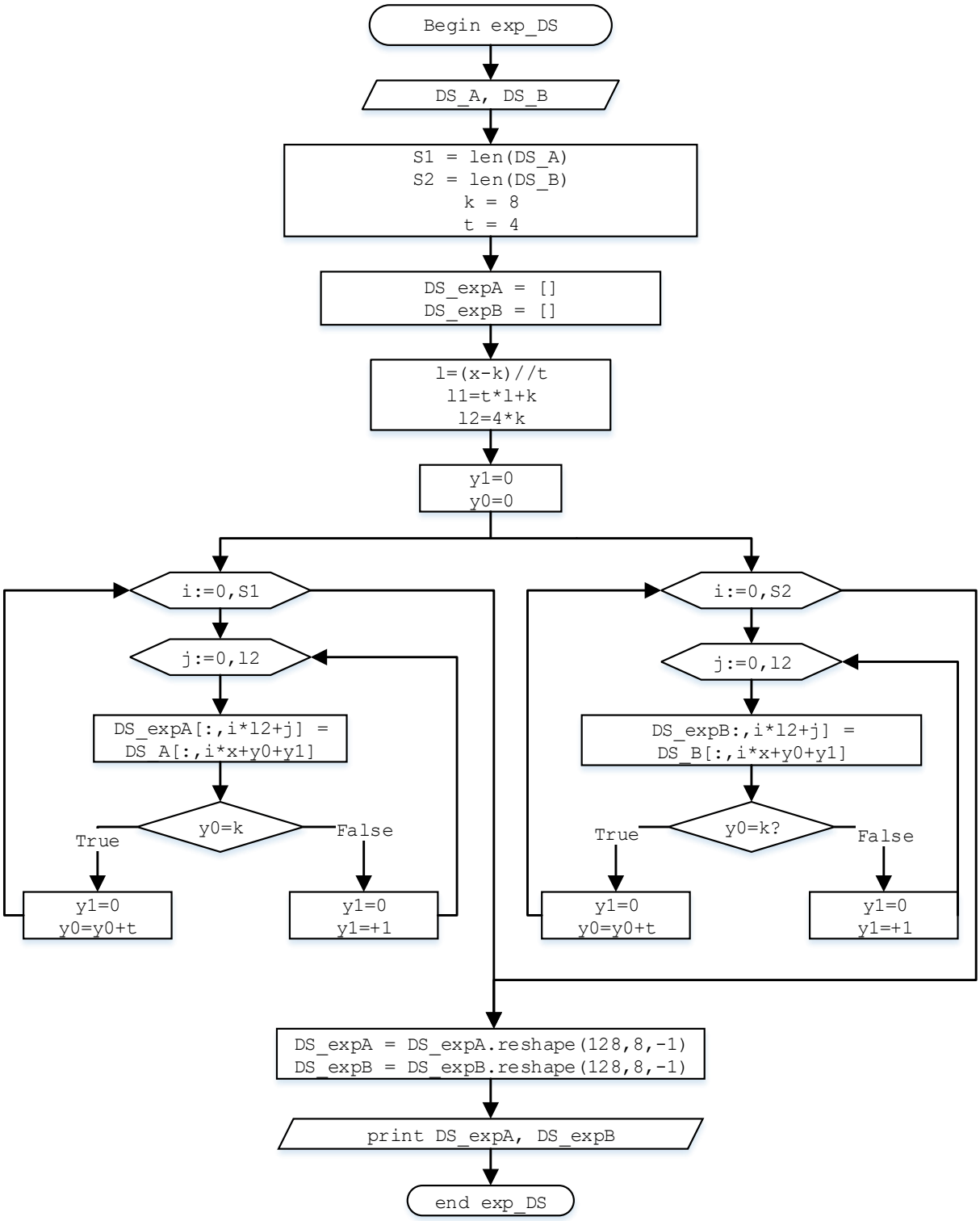

Рис. 4. Блок-схема функции «exp_DS»
Fig. 4. Block diagram of exp_DS function

После формирования полезных для обучения и тестирования массивов DS_expA и DS_expB необходимо объединить их в общий массив DS_X, а также провести процедуру присвоения каждому примеру класса команды соответствующую метку. С данной задачей справляется функция «make_XY», объединяющая данные в единый массив X с присвоением для каждого элемента массива соответствующую метку Y (рисунок 5).

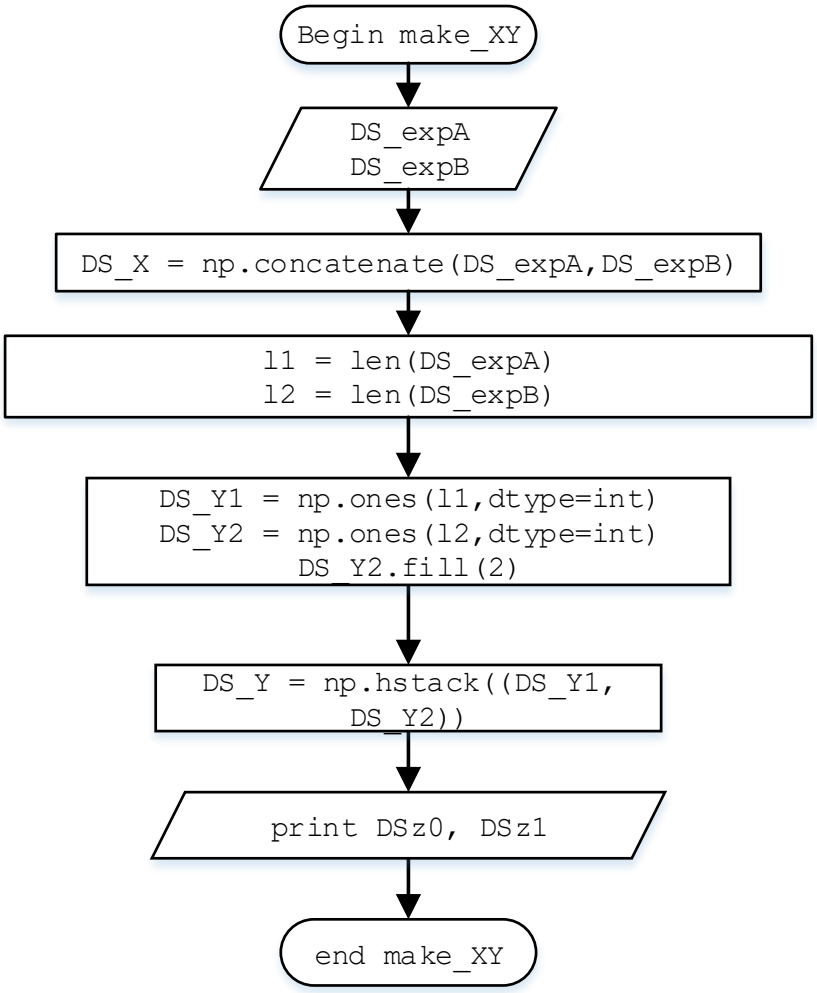

Рис. 5. Блок-схема функции «make_XY»
Fig. 5. Block diagram of make_XY function

В зависимости от длинны соответствующих массивов DS_expA и DS_expB «l1» и «l2», формируются массивы меток DS_Y1 и DS_Y2, где DS_Y1 соответствует метке «сжать» или «1», а DS_Y2 «разжать» или «2». Далее массивы DS_Y1 и DS_Y2 соединяются в единый массив меток DSz1. Выходом функции «make_XY» являются массив команд DSz0 и массив меток DSz1.

Для формирования единого массива команд DS_X соединяются массивы DSz0 и DS_noise11. Для формирования единого массива меток DS_Y соединяются массивы DSz1 и DSy.

Полученные массивы команд и меток, DS_X и DS_Y, были перемешаны между собой в случайном порядке. Для этого была написана функция «mix_XY», которая перемешивает в случайном порядке массив DS_X, и соответственно новому индексу переписывает метку массива DS_Y. Внутри функции генерируется вектор от 0 до «l», размера длинны массива DS_Y, и случайным образом перемешивается. Далее проходя поэлементно массив DS_X и DS_Y внутри цикла, случайное число вектора «r» становится будущим индексом массивов DS_X и DS_Y, перезаписывая их значения в массивы DS_Xmix, DS_Ymix.

Блок-схема функции «mix_XY» представлена на рисунке 6.

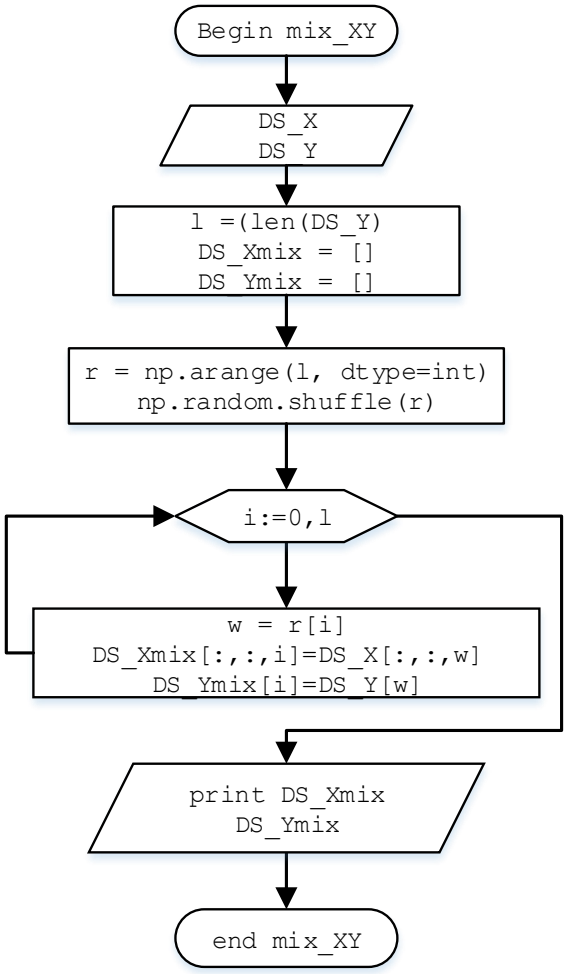

Рис. 7. Блок-схема функции «mix_XY»
Fig. 7. Block diagram of mix_XY function

ЗАКЛЮЧЕНИЕ

В данной статье был разработан алгоритм обработки экспериментальных данных функциональной ближней инфракрасной спектроскопии (fNIRS) головного мозга человека при помощи графического описания алгоритма в виде блок-схем, а также инструментов языка программирования Python. Отличительной особенностью алгоритма является его вариативность и возможность адаптации для типов данных fNIRS с различной частотой снятия данных, а также их размера. Разработанный алгоритм создан для проведения обработки данных, а также формирования наборов данных для обучения и тренировки нейронных сетей глубокого обучения.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-08-01178.

Список литературы

1. Bimodal BCI using simultaneously NIRS and EEG / Y. Tomita, F.B. Vialatte, G. Dreyfus, Y. Mitsukura, H. Bakardjian, A. Cichocki. // IEEE Trans. Biomed Eng. TBME.2014.2300492. – 2014 – No. 61, 1274–1284 pp.
2. Brain–Machine Interfaces in Neurorehabilitation of Stroke / Soekadar, S.R.; Birbaumer, N.; Slutzky, M.W.; Cohen, L.G. // Neurobiol. Dis. 2015, 83, pp.172–179.
3. Comparison of Feature Vector Compositions to Enhance the Performance of NIRS-BCI-Triggered Robotic Hand Orthosis for Post-Stroke Motor Recovery / Jongseung Lee, Nobutaka Mukae, Jumpei Arata, Koji Iihara, Makoto Hashizume // Applied Sciences 2019, 9, 3845; doi:10.3390/app9183845

4. J. ShinNear, K-R. Müller, H-J. Hwang. Near-infrared spectroscopy (NIRS)- based eyes-closed brain-computer interface (BCI) using prefrontal cortex activation due to mental arithmetic // Scientific Reports. 6:36203 – 2016 – 11p.

5. Kaplan A.Ya., Zhigulskaya D.D., Kirjanov D.A. Studying the ability to control human phantom fingers in p300 brain-computer interface // Bulletin of Russian State Medical University .2016. T. 2. C. 24-27.

6. Multichannel-near-InfraredSpectroscopy-Triggered Robotic Hand Rehabilitation System for Stroke Patients / Lee, J.; Mukae, N.; Arata, J.; Iwata, H.; Iramina, K.; Iihara, K.; Hashizume, M. A // IEEE International Conference on Rehabilitation Robotics (ICORR), London, UK, 17–20 July 2017; pp. 158–163.

7. NIRX FNIRS SOFTWARE sistems. URL: https://nirx.net/software (дата обращения:19.05.2020).

8. N. Naseer, K-S. Hong. fNIRS-based brain-computer interfaces: a review // Frontiers in Human Neuroscience – Vol. 9. – 15p.

9. Recognition and classification of oscillatory patterns of electric brain activity using artificial neural network approach / Pchelintseva S.V., Runnova A.E., Musatov V.Y., Hramov A.E. // Proc. SPIE. 2017. V. 10063. DOI: 10.1117/12.2250001

10. Tachtsidis, I.; Scholkmann, F. False Positives and False Negatives in Functional Near-Infrared Spectroscopy: Issues, Challenges, and the Way Forward. Neurophoton 2016, 3, 031405.

References

1. Bimodal BCI using simultaneously NIRS and EEG / Y. Tomita, F.B. Vialatte, G. Dreyfus, Y. Mitsukura, H. Bakardjian, A. Cichocki. // IEEE Trans. Biomed Eng. TBME.2014.2300492. – 2014 – No. 61, 1274–1284 pp.

2. Brain–Machine Interfaces in Neurorehabilitation of Stroke / Soekadar, S.R.; Birbaumer, N.; Slutzky, M.W.; Cohen, L.G. // Neurobiol. Dis. 2015, 83, pp.172–179.

3. Comparison of Feature Vector Compositions to Enhance the Performance of NIRS-BCI-Triggered Robotic Hand Orthosis for Post-Stroke Motor Recovery / Jongseung Lee, Nobutaka Mukae, Jumpei Arata, Koji Iihara, Makoto Hashizume // Applied Sciences 2019, 9, 3845; doi:10.3390/app9183845

4. J. ShinNear, K-R. Müller, H-J. Hwang. Near-infrared spectroscopy (NIRS)- based eyes-closed brain-computer interface (BCI) using prefrontal cortex activation due to mental arithmetic // Scientific Reports. 6:36203 – 2016 – 11p.

5. Kaplan A.Ya., Zhigulskaya D.D., Kirjanov D.A. Studying the ability to control human phantom fingers in p300 brain-computer interface // Bulletin of Russian State Medical University .2016. T. 2. C. 24-27.

6. Multichannel-near-InfraredSpectroscopy-Triggered Robotic Hand Rehabilitation System for Stroke Patients / Lee, J.; Mukae, N.; Arata, J.; Iwata, H.; Iramina, K.; Iihara, K.; Hashizume, M. A // IEEE International Conference on Rehabilitation Robotics (ICORR), London, UK, 17–20 July 2017; pp. 158–163.

7. NIRX FNIRS SOFTWARE sistems. URL: https://nirx.net/software (дата обращения:19.05.2020).

8. N. Naseer, K-S. Hong. fNIRS-based brain-computer interfaces: a review // Frontiers in Human Neuroscience – Vol. 9. – 15p.

9. Recognition and classification of oscillatory patterns of electric brain activity using artificial neural network approach / Pchelintseva S.V., Runnova A.E., Musatov V.Y., Hramov A.E. // Proc. SPIE. 2017. V. 10063. DOI: 10.1117/12.2250001

10. Tachtsidis, I.; Scholkmann, F. False Positives and False Negatives in Functional Near-Infrared Spectroscopy: Issues, Challenges, and the Way Forward. Neurophoton 2016, 3, 031405.

Кононов Виктор Митрофанович, кандидат экономических наук, генеральный директор ООО «ЦентрПрограммСистем»
Асадуллаев Рустам Геннадьевич, кандидат технических наук, доцент, доцент кафедры прикладной информатики и информационных технологий
Щетинина Екатерина Сергеевна, студент кафедры прикладной информатики и информационных технологий
Афонин Андрей Николаевич, доктор технических наук, профессор кафедры материаловедения и нанотехнологий, профессор кафедры информационных и робототехнических систем

Kononov Viktor Mitrofanovich, Candidate of Economical Sciences, General Director of «CentrProgrammSystem», LLC
Asadullaev Rustam Gennadievich, Candidate of Technical Sciences, Associate Professor of the Department of Applied Informatics and Information Technologies
Shchetinina Ekaterina Sergeevna, Bachelor Student, Department of Applied Informatics and Information Technologies
Afonin Andrew Nikolaevich, Doctor of Technical Sciences, Professor of the Department of Materials Science and Nanotechnology, Professor of the Department of Information and Robotic Systems

УДК 004.042 **DOI: 10.18413/2518-1092-2020-5-3-0-5**

Гончаренко Ю.Ю.
Арзамасцев Д.А.

ПРОГРАММНЫЙ МОДУЛЬ ДЛЯ КОНТРОЛЯ И ВЕДЕНИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

Севастопольский государственный университет, ул. Университетская, д. 33, г. Севастополь, 299053, Россия

e-mail: iuliay1985@mail.ru, dan_arz@mail.ru

Аннотация
Электронный документооборот является наиболее быстрым и качественным способом передачи информации на производстве в современных условиях работы. Технология же блокчейн, в свою очередь, может представлять собой надежный механизм для организации информационной безопасности в условиях ведения электронного документооборота, предоставляя значительные преимущества, такие как обеспечение проверки авторства и целостности передаваемых сведений. В статье приведен обзор особенностей ведения электронного документооборота и характеристика технологии блокчейн. Подняты проблемы обеспечения информационной безопасности и законности ведения электронного документооборота и обоснована возможность использования технологии блокчейн для реализации данных целей. Приведены принцип работы технологии блокчейн, описаны проблемы, возможные к возникновению при ее использовании и возможные их решения. Описан алгоритм работы разработанного программного модуля для контроля и ведения электронного документооборота на основе технологии блокчейн с приведением требований для корректной его работы. Разработанное решение имеет преимущества по сравнению с обычной реализацией ведения электронного документооборота, поскольку помимо автоматизации данного процесса является также и механизмом обеспечения информационной безопасности.
Ключевые слова: электронный документооборот; технология блокчейн; информационная безопасность; программная реализация.

UDC 004.042

Goncharenko J.Y.
Arzamastsev D.A.

SOFTWARE MODULE FOR MONITORING AND MAINTAINING ELECTRONIC DOCUMENT MANAGEMENT BASED ON BLOCKCHAIN TECHONOLOGY

Sevastopol state University, 33 Universitetskaya St., Sevastopol, 299053, Russia

e-mail: iuliay1985@mail.ru, dan_arz@mail.ru

Abstract
Electronic document management is the fastest and most high-quality way of transmitting information in production in modern working conditions. Blockchain technology, in turn, can be a reliable mechanism for organizing information security in electronic document management, providing significant advantages, such as providing verification of authorship and the integrity of the information transmitted. The article provides an overview of the features of electronic document management and a characteristic of blockchain technology. The problems of ensuring information security and the legality of electronic document management have been raised and the possibility of using blockchain technology to achieve these goals has been substantiated. The principle of operation of the blockchain technology is described, the problems that may arise during its use and their possible solutions are described. The algorithm of the developed software module for monitoring and maintaining electronic document management based on blockchain technology with requirements for its correct operation is described. The developed solution has advantages compared to the usual implementation of electronic document management, because in addition to automating this process, it is also a mechanism for ensuring information security.

Keywords: electronic document management; blockchain technology; Information Security; software implementation.

ВВЕДЕНИЕ

Электронный документооборот – это явление, получившее в последнее время широкое распространение благодаря значительному упрощению процессов создания, передачи и редактирования информации, как для рядового пользователя персонального компьютера, так и для крупных компаний, предоставляющих свои услуги во всевозможных сферах деятельности, актуальных для современного общества.

Однако, совместно с ростом количества способов возможной передачи информации и развитием методов ее передачи возникают также и существенные риски, касающиеся обеспечения информационной безопасности. До сих пор, например, одним из наиболее часто используемых злоумышленниками вектором атаки является компьютерный взлом, в основном из-за легкости своего осуществления и повышенного интереса к хранимой информации.

Существует множество технологий и способов обеспечения информационной безопасности, однако, в данный момент, интересом в области оказания подобных услуг пользуются практические реализации технологии блокчейн, начавшие пользоваться спросом несколько лет назад и уже доказавшие свою эффективность путем повышения качества жизни множества людей за счет разнообразных применений в большинстве аспектов современной жизни. Например, в настоящее время технология блокчейн активно используются в следующих областях: обеспечение работы криптовалют, смарт-контракты, обеспечение цепочки поставок, регистрация доменных имен; проведение онлайн-голосований, страхование, удостоверение личности [Singh N., 2019]. В июне 2017 года компании Accenture и Microsoft представили систему, реализованную при помощи технологии блокчейн, позволяющую идентифицировать человека и выдать цифровое удостоверение [Accenture, 2017], а уже в мае 2019 года компания Amazon реализовала и открыла собственный сервис, позволяющий клиентам при заключении договора получить собственный сервер и значительно упростить ведение блокчейна. На данный момент, среди их клиентов находятся Philips, Sony Music, Verizon и иные компании [Amazon Web Services, 2018].

Учитывая подобный стремительный рост использования данной технологии и широту спектра ее возможного применения, она способна не только обеспечить повышение информационной безопасности данных, но также и рост уровня оказываемых услуг, предоставляя пользователям большое количество возможностей своего использования.

ОСОБЕННОСТИ ВЕДЕНИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ БЛОКЧЕЙН

Электронный документооборот – это обмен электронными документами по доступным каналам связи, как внутри предприятия, так и вне его [DOCFLOW, 2017].

Электронный документ – это файл или любая иная информация, представленная в цифровом виде, хранящаяся/передающаяся в пределах какой-либо информационной системы.

Понятия электронного документооборота или электронного документа не приводятся в нормативно-правовых документах, однако активно используются, что показывает распространенность и удобство в освоении электронного документооборота и может послужить доказательством его активного использования в практических вопросах.

К нормативно-правовым документам, регулирующим вопросы электронного документооборота можно отнести Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» и Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи», поскольку в них описываются основные понятия данного вопроса, такие как «информация», способы ее передачи и регулируются требования к электронной цифровой подписи, позволяющие организовывать электронный документооборот на предприятии [Информационная система 1С:ИТС, 2020].

Документом, обеспечивающим законность ведения электронного документооборота при условии подписания сообщений электронной цифровой подписью, является Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи». А именно, в статье 7 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» «Признание электронных подписей, созданных в соответствии с нормами иностранного права и международными стандартами» приведено нижеследующее.

Электронные подписи, созданные в соответствии с нормами права иностранного государства и международными стандартами, в Российской Федерации признаются электронными подписями того вида, признакам которого они соответствуют на основании Федерального закона [КонсультантПлюс, 2020].

Электронная подпись и подписанный ею электронный документ не могут считаться не имеющими юридической силы только на том основании, что сертификат ключа проверки электронной подписи выдан в соответствии с нормами иностранного права [КонсультантПлюс, 2020].

Для обеспечения реализации этих целей также может использоваться и технология блокчейн, поскольку способна обеспечить проверку авторства и целостности любых данных или документа, передающихся в сети.

Блокчейн – это цепочка блоков информации заранее определенного содержания, созданных по заранее определенных правилам или любых других записей, сообщений или сведений, необходимых для сохранения, передачи и просмотра [Блокчейн, 2020].

Один блок блокчейна является специальной структурой, созданной для хранения сведений об одном, или любом другом, определенном заранее, количестве событий, сообщений или любом другом представлении определенной информации. Содержимое любого блока блокчейна всегда может быть просмотрено, а информация проверена на подлинность путем сравнения с информацией, представленной в соответствующем блоке блокчейна.

Каждый блок блокчейна, кроме родительского, необходимого только лишь для поддержания работоспособности технологии, содержит в себе информацию заранее определенного содержания, в зависимости от необходимости применения технологии, области ее применения и иных факторов. Однако, в независимости от перечисленных факторов, в блоке всегда присутствует следующая информация:

- номер блока;
- хеш предыдущего блока;
- информация для сохранения;
- хеш данного блока [Щербань Е, 2017].

У данной технологии существует лишь одна проблема, возникающая в ходе ее использования, а именно – проблема возникновения параллельных ветвей, что означает создание последовательности блоков блокчейна, состоящей из одного или более блока, продолжающейся путем добавления в блокчейн блоков к блоку главной ветви. Такие ветви, как правило, образуются при желании злоумышленников изменить представление остальных пользователей сети об информации, находящейся в одном из блоков блокчейна для достижения личных целей [Hooda P., 2020].

Данная проблема, однако, легко решается на практике путем использования механизмов защиты таких как PoW (Proof of Work) (доказательство работой), PoB (Proof of Burn) (доказательство уничтожением), PoS (Proof of Stake) (доказательство долей), PoC (Proof of Capacity) (доказательство объемом), PoET (Proof of Elapsed Time) (доказательство затраченным временем) или простым игнорированием возможной параллельной ветви иными пользователями сети [Sharma T., 2018].

Таким образом, технология блокчейн является крайне гибкой технологией, доступной к реализации для решения огромного спектра задач и способна значительно упростить некоторые процессы и аспекты жизни человека, а некоторые – существенно улучшить путем решения

множества современных проблем, в том числе и за счет обеспечения информационной безопасности.

ОПИСАНИЕ РАБОТЫ ПРОГРАММНОГО МОДУЛЯ

Разработанный программный модуль для контроля и ведения электронного документооборота на основе технологии блокчейн позволяет обеспечить реализацию электронного документооборота в локальной сети, поддерживая передачу и обеспечение целостности сообщений и передаваемых файлов, также обеспечивая проверку авторства.

Для корректной работы программного модуля на компьютере конечного пользователя должен быть установлен язык программирования Python версии 3.7.1 или более и следующие модули данного языка:

- socket;
- threading;
- os;
- hashlib;
- ntplib;
- time;
- datetime;
- easygui.

Модуль socket позволяет в ходе работы программы создавать сокеты (начальные или конечные точки коммуникации) из пары значений IP-адреса и сетевого порта компьютера, производить подключения и передавать данные между ними.

Модуль threading позволяет в ходе работы программы создавать или удалять раздельные потоки выполнения программного кода, обеспечивая таким образом многопоточность программы, значительно сокращая время ее выполнения.

Модуль os позволяет в ходе работы программы обеспечить возможность выполнения базовых функций операционной системы путем вызова соответствующих команд в командной строке.

Модуль hashlib позволяет в ходе работы программы обеспечить выполнение криптографических хеш-функций, указывая входные данные и получая выходные данные соответствующих алгоритмов хеширования.

Модуль ntplib позволяет в ходе работы программы получить точное время, включая доли секунд, для различных часовых поясов путем формирования и отправки запроса к проекту Network Time Protocol и получения ответа в виде метки времени.

Модуль time позволяет в ходе работы программы получить сведения о текущих времени и дате, используя системные часы, а также приостановить работу программы на определенный промежуток времени путем вызова функции sleep, для чего, как правило, и используется, обеспечивая, например, определенный период ожидания в ходе выполнения программы для сохранения ресурсов.

Модуль datetime позволяет в ходе работы программы, как и модуль time, получить сведения о текущих времени и дате, используя системные часы, однако предоставляет гораздо более расширенный функционал для выполнения различного спектра задач, а также позволяет изменять формат меток времени, предоставляя их более понятным для восприятия путем.

Модуль easygui позволяет в ходе работы программы обеспечить создание, появление и сбор данных через элементы графического интерфейса, что способствует более комфортному использованию программы конечным пользователем.

Модули socket, threading, os, hashlib, time и datetime поставляются совместно с языком программирования Python, однако модули ntplib и easygui должны быть установлены перед началом работы программы путем выполнения команды «python –m pip install ntplib» в командной строке операционной системы.

Помимо этого, рекомендуется полученный исполняемый файл поместить в любую директорию, изначально не содержащую в себе папку «files» и файлы chain.txt и tempchain.txt, иначе файлы будут перезаписаны, а в папка «files» будет в дальнейшем использоваться как служебная папка программы.

При разработке программного модуля были учтены вопросы обеспечения информационной безопасности при работе с технологией блокчейн. Из-за этого, при любом обнаружении несоответствия уже имеющихся данных в блокчейне пользователя в сравнении его с блокчейном другого пользователя это будет свидетельствовать о возникновении параллельной ветви блокчейна, что может подразумевать появление злоумышленника в локальной сети. Участник сети с различающимся блокчейном не сможет передать его иному пользователю ни при каких обстоятельствах, а пользователю, инициировавшему проверку или обновление блокчейна, будь это любой из этих пользователей в ближайшем диалоговом окне будет рекомендовано обратиться к вышестоящему лицу.

В начале своего выполнения разработанный программный модуль подключает библиотеки, необходимые для его работы, и представляет пользователю поочередно два диалоговых окна, предназначенных для ввода локального IP-адреса компьютера пользователя и для ввода IP-адресов иных компьютеров в локальной сети, проверяет наличие папки «files» и файла chain.txt и, в случае их отсутствия создает их. Далее выполняется основной цикл программы.

Выполнение основного цикла программы сопровождается появлением главного меню программного модуля. При первом выполнении цикла главное меню, помимо основного текста, будет содержать следующий: «Рекомендуемая операция: обновить блокчейн», тогда как при последующих выполнениях (после первого выбора операции пользователем) главное меню будет содержать только основной текст: «Пожалуйста, выберите необходимую операцию:» (рис. 1).

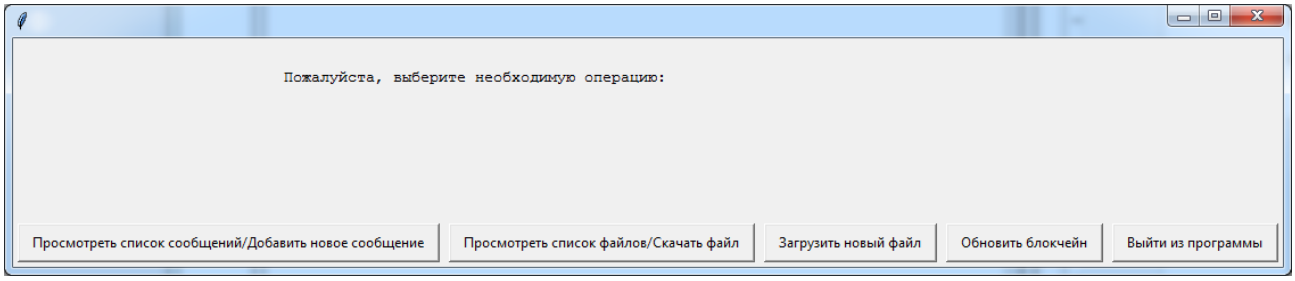

Рис. 1. Главное меню программного модуля
Fig. 1. The main menu of the software module

При выборе пользователем опции «Просмотреть список сообщений/Добавить новое сообщение» из главного меню, возникнет окно сообщений, содержащее текст «К сожалению, никто еще не добавлял сообщения» или список сообщений с указанием локального IP-адреса компьютера отправителя каждого сообщения. Окно сообщений всегда будет содержать опции «Добавить новое сообщение» и «Вернуться в главное меню» (рис. 2).

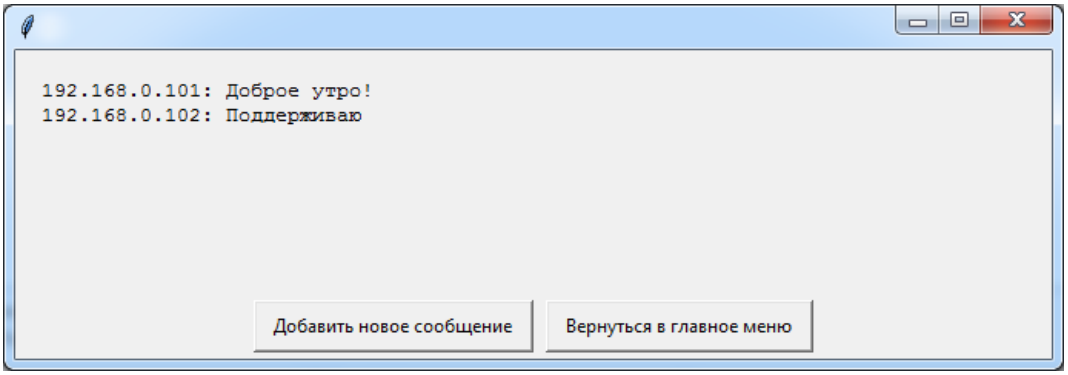

Рис. 2. Окно сообщений
Fig. 2. Message window

При выборе пользователем опции «Добавить новое сообщение» возникнет диалоговое окно с полем для ввода сообщения. После ввода сообщения пользователем блокчейн будет обновлен и разослан всем участникам сети, чьи локальные IP-адреса были указаны ранее. После добавления сообщения в блокчейн или при выборе пользователем на любом этапе опции отмены произойдет возврат в главное меню.

При выборе пользователем опции «Просмотреть список файлов/Скачать файл» из главного меню, возникнет диалоговое окно, содержащее список файлов, когда-либо добавленных в блокчейн всеми пользователями сети с указанием локального IP-адреса компьютера, хранящего файл (рис. 3).

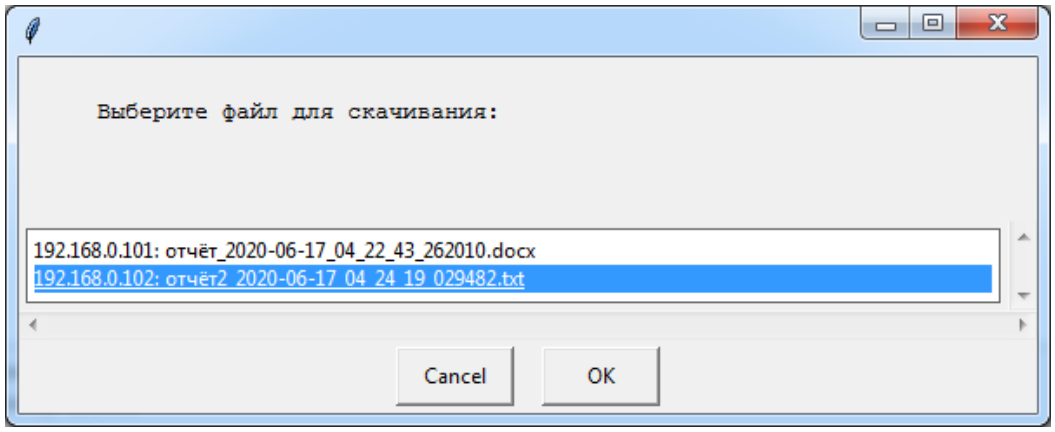

Рис. 3. Окно со списком файлов
Fig. 3. Window with a list of files

При выборе пользователем файла для скачивания возникнет диалоговое окно, предлагающее выбрать имя и путь для сохранения файла, далее произойдет подключение к компьютеру, хранящему данный файл и его загрузка. В случае, если файл, выбранный пользователем изначально был загружен им же возникнет диалоговое окно, предлагающее продолжить или отменить загрузку файла. В случае выбора пользователем варианта продолжить загрузку файл будет скопирован из служебной папки «files».

Результаты загрузки файла будут показаны пользователю в дальнейшем диалоговом окне. После загрузки файла или при выборе пользователем на любом этапе опции отмены произойдет возврат в главное меню.

При выборе пользователем опции «Загрузить новый файл» из главного меню, возникнет диалоговое окно, предлагающее выбрать пользователю файл для добавления его в блокчейн. После выбора файла произойдет его копирование в служебную папку «files», с дальнейшем добавлением информации об этом файле в блокчейн и рассылке блокчейна всем пользователям сети.

При выборе пользователем опции «Обновить блокчейн» из главного меню, произойдет процесс обновления блокчейна пользователя, который подразумевает нахождение иного пользователя локальной сети с длиннейшим файлом блокчейна и копирование информации из него. Однако, если уже имеющиеся данные в блокчейне пользователя, запросившего обновление, различны обновления блокчейна не произойдет. После выполнения данного процесса возникнет диалоговое окно, уведомляющее пользователя об обновлении или причинах невозможности обновления его блокчейна (рис. 4).

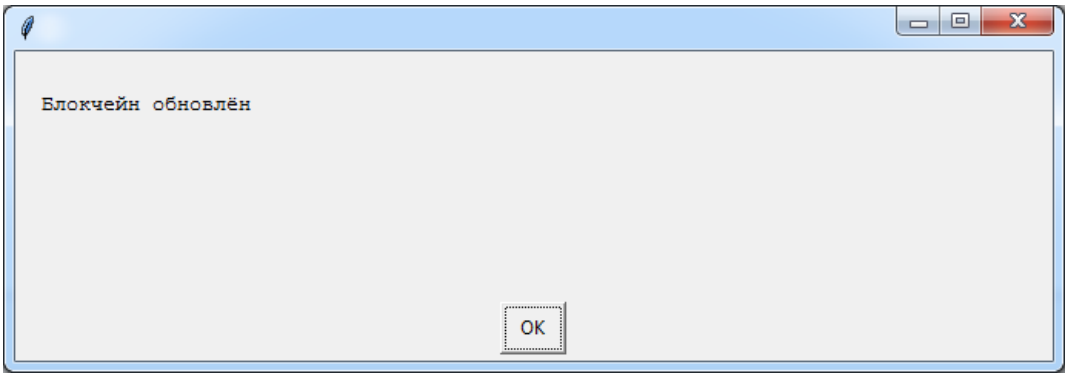

Рис. 4. Успешное обновление блокчейна
Fig. 4. Successful blockchain update

При выборе пользователем опции «Выйти из программы» из главного меню, произойдет ожидание завершения всех параллельных потоков, созданных в процессе работы программы и завершение работы основного цикла программы, что приведет к выходу из нее.

В ходе работы программы при рассылке блокчейна после добавления в него каких-либо данных всегда возникнет окно, содержащее результаты рассылки блокчейна для всех пользователя сети с указанием их IP-адресов и соответствующих результатов (рис. 5).

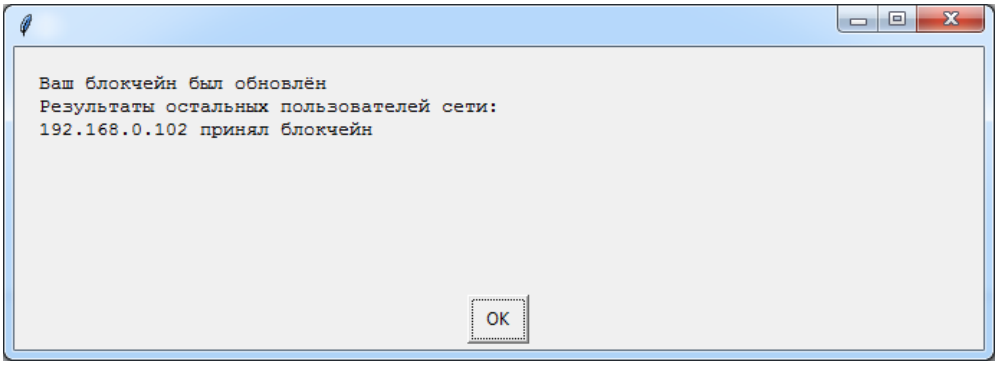

Рис. 5. Окно с результатами рассылки блокчейна
Fig. 5. Window with the results of blockchain distribution

Помимо этого, в ходе работы программы при успешном обновлении блокчейна, если инициатором обновления являлся другой пользователь сети, вне зависимости от текущего этапа выполнения программы всегда возникнет окно, уведомляющее об обновлении блокчейна.

Пример файла блокчейна, дополнявшегося записями в ходе работы программного модуля представлен на рисунке 6.

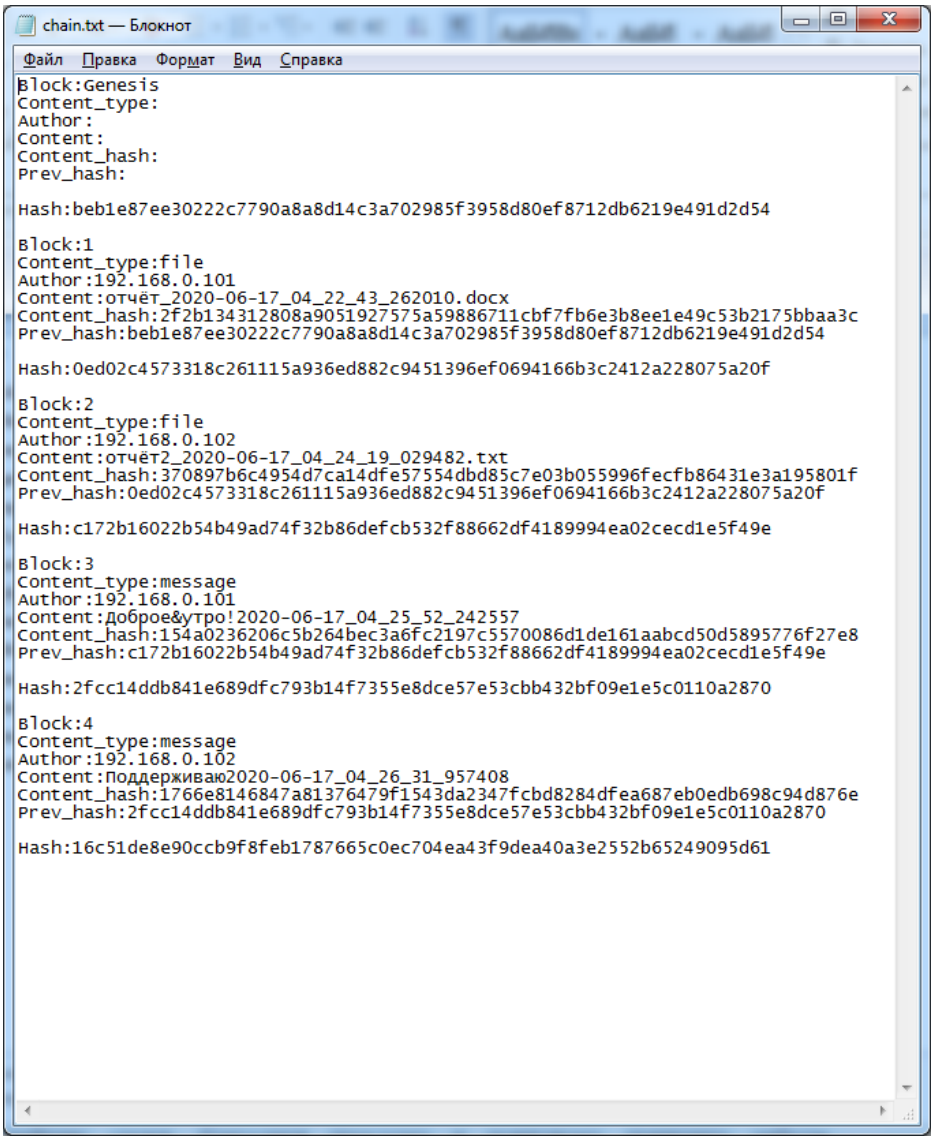

Рис. 6. Файл блокчейна
Fig. 6. Blockchain file

ЗАКЛЮЧЕНИЕ

Таким образом, разработанный программный модуль для контроля и ведения электронного документооборота на основе технологии блокчейн обладает возможностями значительно ускорить процесс передачи информации в сети, убедиться в ее получении иными пользователями сети и способен предоставить должный уровень защиты информации при ведении электронного документооборота за счет использования преимуществ технологии блокчейн.

Список литературы

1. Блокчейн, 2020. URL: https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD (дата обращения: 02.05.2020).
2. Информационная система 1С: ИТС, 2020. Правовые основы обмена электронными документами. URL: https://its.1c.ru/db/eldocs#content:3:hdoc (дата обращения: 01.05.2020).
3. КонсультантПлюс, 2020. Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=354532 (дата обращения: 01.05.2020).
4. Щербань Е, 2017. Что такое блокчейн, и как это работает. URL: https://revolverlab.com/how-its-works-blockchain-6d0355c43bfc (дата обращения: 03.06.2020).

5. DOCFLOW, 2017. Электронный документооборот: что такое электронный документооборот, основные понятия, виды, преимущества, задачи, критерии выбора, классификация систем, требования. URL: http://www.docflow.ru/edu/glossary/detail.php?ID=27946 (дата обращения: 01.06.2020).
6. Accenture, 2017. Accenture, Microsoft Create Blockchain Solution to Support ID2020. URL: https://newsroom.accenture.com/news/accenture-microsoft-create-blockchain-solution-to-support-id2020.htm (дата обращения: 04.05.2020).
7. Amazon Web Services, 2018. Amazon Managed Blockchain. URL: https://aws.amazon.com/ru/managed-blockchain/ (дата обращения: 04.05.2020).
8. Hooda P., 2020. Blockchain Forks. URL: https://www.geeksforgeeks.org/blockchain-forks/ (дата обращения: 03.05.2020).
9. Singh N., 2019. Blockchain Usage: List of 20+ Blockchain Technology Use Cases. URL: https://101blockchains.com/blockchain-usage/ (дата обращения: 04.05.2020).
10. Sharma T., 2018. What are the alternative strategies for Proof-Of-Work? URL: https://www.blockchain-council.org/blockchain/what-are-the-alternative-strategies-for-proof-of-work/ (дата обращения: 04.05.2020).

References

1. Blockchain, 2020. URL: https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD (access date: 02/06/2020).
2. Information system 1C: ITS, 2020. Legal basis for the exchange of electronic documents. URL: https://its.1c.ru/db/eldocs#content:3:hdoc (access date: 01/06/2020).
3. ConsultantPlus, 2020. Federal Law of 06.04.2011 N 63-ФЗ «On electronic signature». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=354532 (access date: 01/06/2020).
4. Shcherban E, 2017. What is blockchain and how does it work. URL: https://revolverlab.com/how-its-works-blockchain-6d0355c43bfc (access date: 03/06/2020).
5. DOCFLOW, 2017. Electronic document management: what is electronic document management, basic concepts, types, advantages, tasks, selection criteria, classification of systems, requirements. URL: http://www.docflow.ru/edu/glossary/detail.php?ID=27946 (access date: 01/06/2020).
6. Accenture, 2017. Accenture, Microsoft Create Blockchain Solution to Support ID2020. URL: https://newsroom.accenture.com/news/accenture-microsoft-create-blockchain-solution-to-support-id2020.htm (access date: 04/06/2020).
7. Amazon Web Services, 2018. Amazon Managed Blockchain. URL: https://aws.amazon.com/ru/managed-blockchain/ (access date: 04/06/2020).
8. Hooda P., 2020. Blockchain Forks. URL: https://www.geeksforgeeks.org/blockchain-forks/ (access date: 03/06/2020).
9. Singh N., 2019. Blockchain Usage: List of 20+ Blockchain Technology Use Cases. URL: https://101blockchains.com/blockchain-usage/ (access date: 04/06/2020).
10. Sharma T., 2018. What are the alternative strategies for Proof-Of-Work? URL: https://www.blockchain-council.org/blockchain/what-are-the-alternative-strategies-for-proof-of-work/ (access date: 04/06/2020).

Гончаренко Юлия Юрьевна, доктор технических наук, доцент, профессор кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности
Арзамасцев Даниил Аркадиевич, студент кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности

Goncharenko Julia Yurievna, Doctor of Technical Sciences, Associate Professor, Professor of the Department Information security, Institute of Radioelectronics and Information Security
Arzamastsev Daniil Arkadievich, student of the Department Information security, Institute of Radioelectronics and Information Security

УДК 004.9 **DOI: 10.18413/2518-1092-2020-5-3-0-6**

Ильинская Е.В.
Скрипина И.И.

АНАЛИЗ НАИБОЛЕЕ АКТУАЛЬНЫХ ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ ОЦЕНКИ РИСКОВ ПРИ ПРОЕКТИРОВАНИИ ИНФОРМАЦИОННЫХ СИСТЕМ

Белгородский государственный национальный исследовательский университет, ул. Победы, д. 85, г. Белгород, 308015, Россия

e-mail: chmireva@bsu.edu.ru, skripina@bsu.edu.ru

Аннотация
В настоящее время проекты все более неопределенны уже на первых стадиях проектирования и сопровождаются большим количеством рисков. В статье рассматриваются инструментальные средства оценки рисков при проектировании информационных систем, такие как: CRAMM, RiskWatch и ГРИФ, проводится их краткое описание и сравнительный анализ. При проведении сравнительного анализа особое внимание уделяется следующим критериям: легкость работы для пользователя, стоимость лицензии за одно рабочее место, функциональность, функция ущерба.
Ключевые слова: риск при проектировании информационных систем; инструментальные средства оценки рисков; CRAMM; RiskWatch; ГРИФ.

UDC 004.9

Ilinskaja E.V.
Skripina I.I.

ANALYSIS OF THE MOST ACTUAL INSTRUMENTAL TOOLS FOR RISK ASSESSMENT IN DESIGNING INFORMATION SYSTEMS

Belgorod State National Research University, 85 Pobedy St., Belgorod, 308015, Russia

e-mail: chmireva@bsu.edu.ru, skripina@bsu.edu.ru

Abstract
Currently, projects are increasingly uncertain in the early stages of design and are accompanied by a large number of risks. The article discusses the tools for risk assessment in the design of information systems, such as: CRAMM, RiskWatch and GRIF, provides a brief description and comparative analysis. When conducting a comparative analysis, special attention is paid to the following criteria: ease of work for the user, the cost of a license for one workplace, functionality, damage function.
Keywords: risk in the design of information systems; risk assessment tools; CRAMM; RiskWatch; GRIF.

Проектирование информационных систем является очень долгосрочным и трудозатратным процессом, включающим в себя несколько этапов, который, как правило, связан с большим количеством сопутствующих рисков. В настоящее время проекты все более неопределенны уже на первых стадиях проектирования и сопровождаются большим количеством рисков.

В зависимости от сферы деятельности понятие «риск» может трактоваться по-разному, в этой связи существуют разные определения риска как категории. Обзор и анализ экономической литературы [3, 4], стандартов по управлению рисками [2] позволил сформулировать наиболее полный, на наш взгляд, подход к понятию «риск». Риск в проектной практике представляет собой вероятность возникновения неблагоприятных событий и их последствий, которые могут оказать влияние на успех реализации проекта и привести к возникновению финансовых потерь.

Рассмотрим наиболее актуальные инструментальные средства оценки рисков, которые могут быть использованы для оценки рисков при проектировании информационных систем:

- CRAMM;
- RiskWatch;
- Гриф.

Инструментальное средство CRAMM разработано британской компанией Insight Consulting [4].

Отличительной особенностью, характеризующей метод с положительной стороны, является системный комплексный подход, учитывающий количественную и качественную оценку рисков. При использовании инструментального средства CRAMM описываются защищаемые ресурсы с финансовой точки зрения в их денежном выражении, далее вычисляется необходимый показатель защиты проектируемой системы исходя из ценности защищаемой информации. На следующем шаге выполняется качественная и количественная оценка наступления рисковых событий для всех ресурсов, а также вычисляется уровень рисковых событий, далее применяются классические инструкции в зависимости от уровня рисковых событий и необходимого уровня защиты конкретного ресурса. В настоящее время пользователями инструментального средства CRAMM являются аудиторы со специальной подготовкой. Существует возможность использования богатой базы с готовыми примерами применения метода для множества ресурсов различных проектов.

Интерфейс инструментального средства CRAMM представлен на рисунке 1.

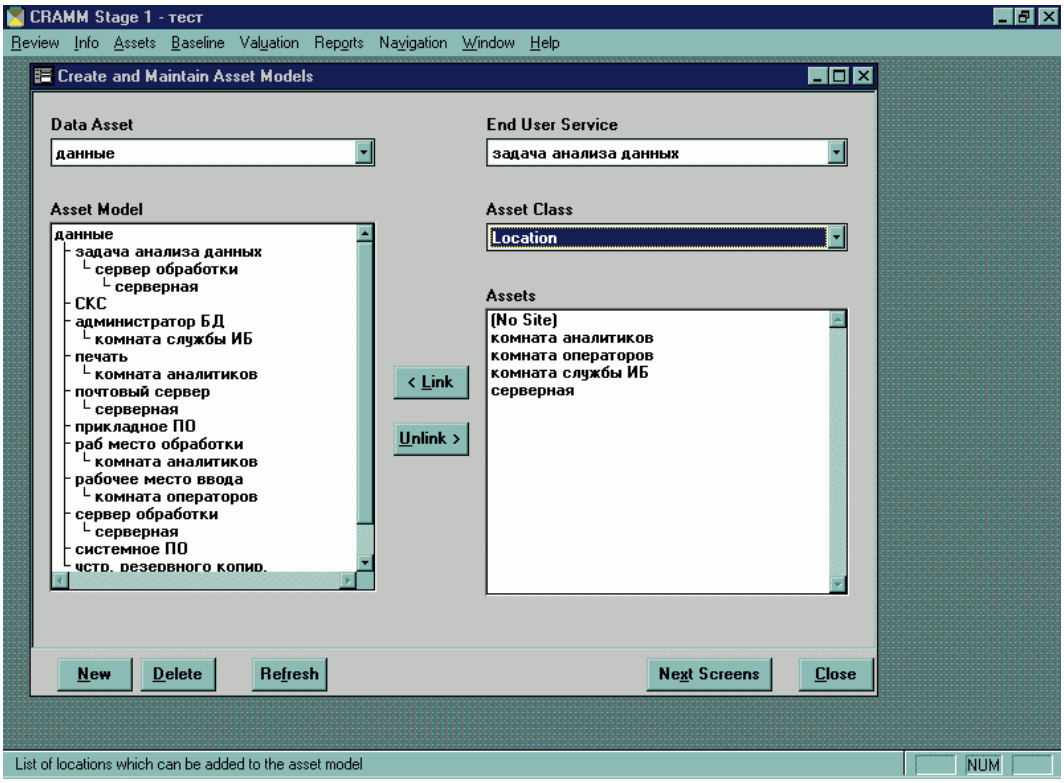

Рис. 1. Инструментальное средство CRAMM
Fig. 1. The CRAMM software tool

Рассмотрим недостатки инструментального средства CRAMM. Важным недостатком применения указанного средства является необходимость привлечения внешних аудиторов. Помимо этого, нужно учитывать, что инструментальное средство CRAMM применяется для проведения оценки рисков у уже внедренных информационных систем, а для оценки рисков при проектировании информационных систем он не предназначен. Инструментальное средство CRAMM разработано британской компанией и не маловажным недостатком является отсутствие русскоязычной версии данного средства.

Рассмотри инструментальное средство RiskWatch. Данное средство разработано компанией под названием RiskWatch Inc (США) для осуществления анализа и оценки различных видов рисков [5]. Отличительной чертой по сравнению с инструментальным средством CRAMM является ориентированность на идентификацию всех возможных рисков на первых стадиях проектирования информационной системы. Инструкции система выдает, опираясь на

утверждение, что финансовые затраты на управление возможными рисками не должны превышать сумму убытков от наступления какого-либо из идентифицированных рисков. На начальном этапе выявляются кластеры возможных рисков, далее просчитываются все возможные финансовые и другие убытки и классы неблагоприятных событий. Для достижения этой цели применяется специализированный опросник. Он содержит обширную базу данных с вопросами различных видов. В результате анализа ответов на вопросы опросника появляется возможность достаточно полно и четко идентифицировать риски, возникающие при проектировании информационной системы. На заключительном этапе выявляются взаимосвязи между убытками и рисковыми событиями. На основе полученных данных выполняется количественная оценка возможных убытков и генерируются инструкции по определенным мероприятиям предотвращения наступления риска.

Интерфейс инструментального средства RiskWatch представлен на рисунке 2.

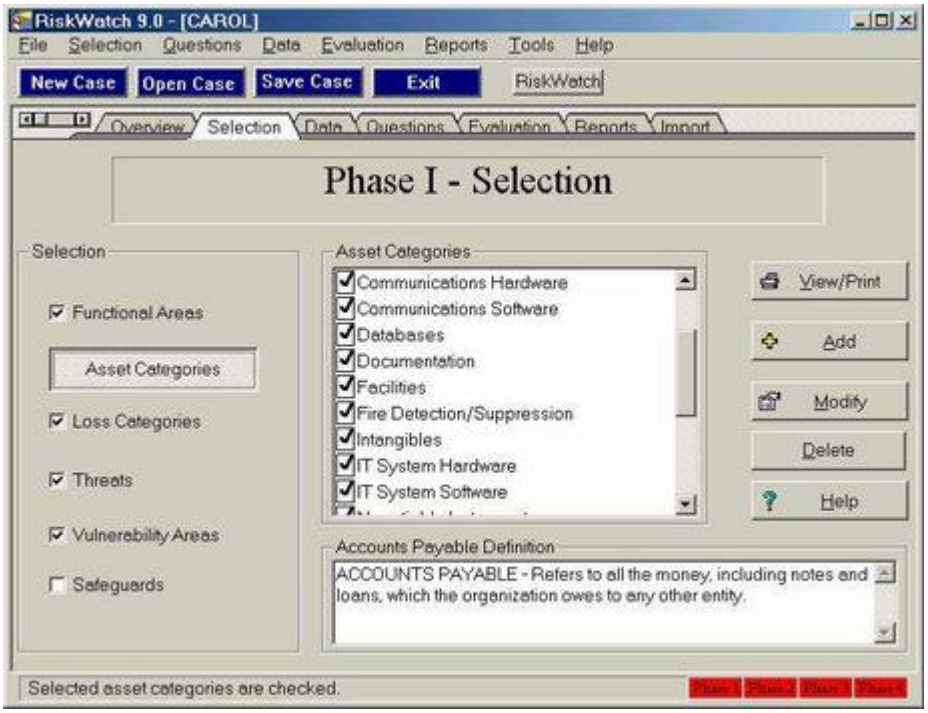

Рис. 2. Инструментальное средство RiskWatch
Fig. 2. The RiskWatch software tool

Использование инструментального средства RiskWatch позволяет количественно оценить вероятность наступления рисковых событий. На основе полученных результатов оценки можно судить о рентабельности проектирования и разработки информационной системы.

Инструментальное средство RiskWatch RiskWatch обладает некоторыми недостатками, в их числе: сложность проведения мониторинга, неинформативные инструкции по использованию информационных средств обеспечения защиты от наступления различных рисков, сложность, связанная с применением программы русскоязычными пользователями на английском языке.

Аналогом рассмотренных зарубежных инструментальных средств является отечественная русскоязычная программа ГРИФ (компания-разработчик Digital Security) [5]. В функционал программы входят анализ бизнес-процессов, оценка наступления возможных рисковых событий.

Инструментальное средство ГРИФ имеет интуитивно понятный для пользователя интерфейс, который представлен на рисунке 3.

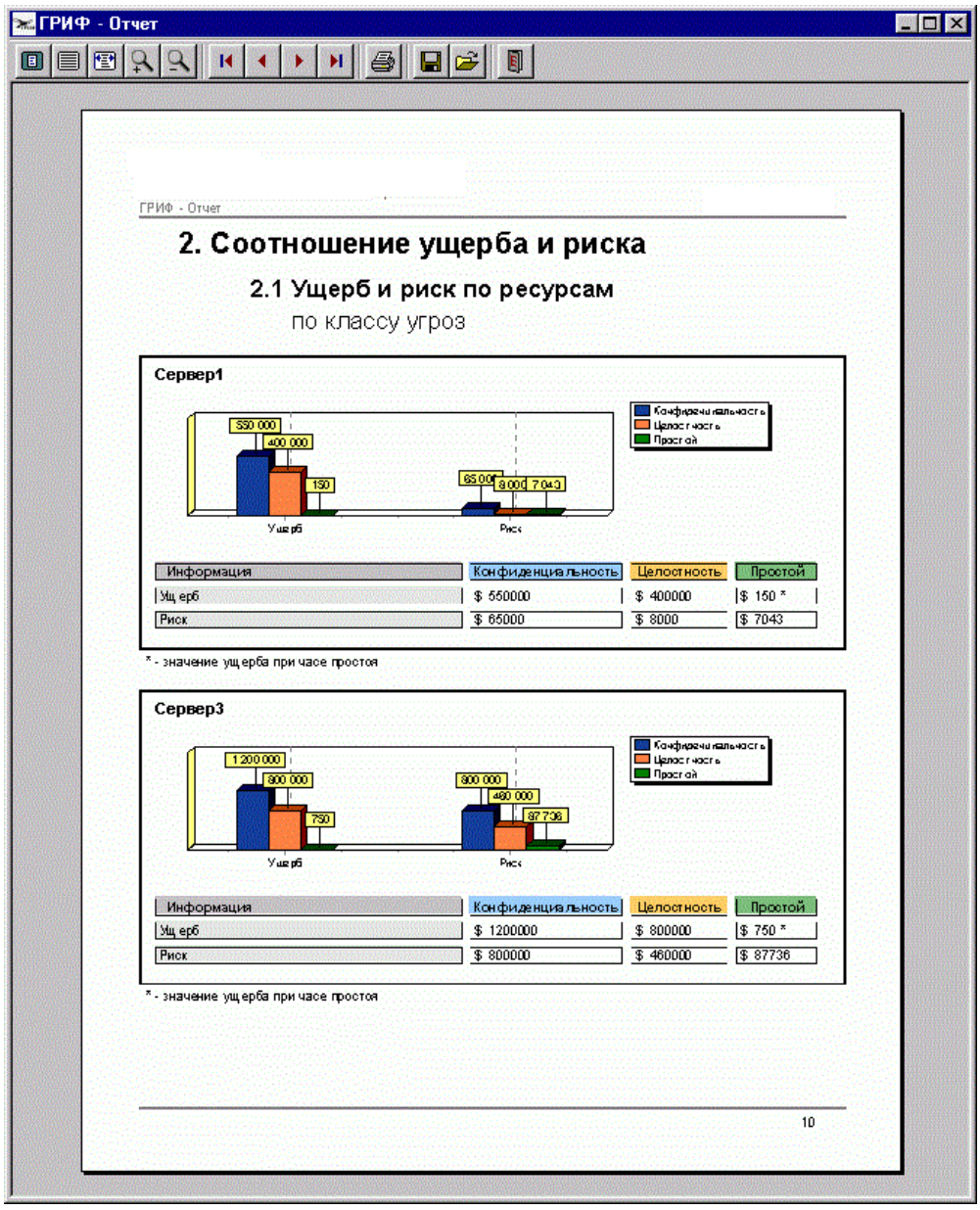

Рис. 3. Инструментальное средство ГРИФ
Fig. 3. The GRIF software tool

К достоинствам инструментального средства ГРИФ относят возможность анализа бизнес-процессов, на основе которого выполняется построение функциональной модели. Модель содержит описание информационных ресурсов, информацию о пользователях, а также сведения о средствах предотвращения наступления рисковых событий. С помощью инструментального средства ГРИФ на основе полученной модели выводится карта взаимосвязей пользователей и ресурсов в исследуемой информационной системе. На следующем этапе выполняется операция установления необходимости применения используемой политики безопасности в соответствии с архитектурой информационной системы. Выполняется это подобно тому, как и в инструментальном средстве RiskWatch, при помощи специализированных опросников с большой базой данных с вопросами. Далее производится анализ и оценка вероятности наступления рисковых событий. Выявляются все возможные угрозы и риски на каждом этапе жизненного цикла проекта. На основе полученных данных выполняется построение обновленной модели с применением математико-статистического моделирования. На завершающем этапе инструментальное средство выдает рекомендации по определенным мероприятиям предотвращения наступления риска.

Инструментальное средство ГРИФ обладает рядом достоинств и преимуществ по сравнению со своими аналогами, в их числе: мониторинг динамики бизнес-процессов, анализ политики безопасности в соответствии с архитектурой информационной системы. Есть и отрицательные черты у рассматриваемого средства, это небольшая база решений, что может повлиять на длительность и цену анализа рисков при проектировании информационных систем. Еще одним недостатком является необходимость обучения использования инструментального средства ГРИФ.

Сравнительные характеристики рассмотренных инструментальных средств приведены в таблице (таблица 1).

Таблица 1

Сравнительная характеристика инструментальных средств анализа рисков

Table 1

Comparative analysis of risk analysis tools

Критерии сравнения	**CRAMM**	**RiskWatch**	**ГРИФ**
Страна-разработчик	Великобритания	США	Россия
Наличие поддержки	+	+	+
Функционал	Входные данные: – ресурсы; – ценность ресурсов; – угрозы; – уязвимости системы; – выбор адекватных контрмер.	Входные данные: – тип информационной системы; – базовые требования в области безопасности; – ресурсы; – потери; – угрозы; – меры защиты.	Входные данные: – ресурсы; – сетевое оборудование; – виды информации; – группы пользователей; – средства защиты; – угрозы; – уязвимости.
Простота использования	-	-	+
Стоимость лицензии, $	От 2000 до 5000	От 10 000	От 1000
Метод оценки	Качественная оценка	Количественная оценка	Качественная и количественная оценки
Корпоративная версия	-	-	+
Задание ущерба	Как следствие нарушения свойств активов	Как следствие реализации угроз	Как следствие нарушения свойств активов
Функция ущерба	Для свойств доступности зависит от времени. Для свойств конфиденциальности целостности постоянна	Постоянна, не зависит от времени	Для свойств доступности зависит от времени. Для свойств конфиденциальност и целостности постоянна
Недостатки	1) Требует специализированных компетенций у пользователя. 2) Подходит для	1) Не учитывает организационный фактор. Оценка рисков, произведённая с	1) Нет возможности сравнения отчетов на разных этапах внедрения комплекса мер по

Критерии сравнения	CRAMM	RiskWatch	ГРИФ
	разработанных информационных систем, не учитывает особенности на этапе проектирования. 3) Огромное количество отчетов.	помощью инструментального средства, не является комплексной.	обеспечению защищенности 2) Отсутствие возможности добавления специфичных для разных сфер деятельности требований политики безопасности.

Проанализировав таблицу 1, можно сделать вывод, что среди рассмотренных инструментальных средств самым универсальным и подходящим под потребности российских пользователей является инструментальное средство ГРИФ. Оно позволяет проводить мониторинг динамики бизнес-процессов, анализ политики безопасности в соответствии с архитектурой информационной системы. У ГРИФ самая невысокая цена по сравнению с другими, оно не требуют наличия специализированных компетенций у пользователей, реализовано на русском языке.

Список литературы

1. Асадуллаев, Р.Г. Разработка средств оценки проектных рисков при создании информационных систем для сферы государственных услуг [Текст] / Р.Г. Асадуллаев, В.В. Ломакин, Н.П. Путивцева, О.С. Резниченко, Ю.Ю. Белоконь // Научно-технический вестник Поволжья, 2017. – № 5. – С. 120-122.

2. Воронцовский, А.В. Управление рисками: Учебник и практикум для бакалавриата и магистратуры [Текст] / А.В. Воронцовский. – Люберцы: Юрайт, 2016. – 414 с.

3. Домащенко, Д.В. Управление рисками в условиях финансовой нестабильности [Текст] / Д.В. Домащенко, Ю.Ю. Финогенова. – М.: Магистр, ИНФРА-М, 2010. – 238 с.

4. Гнедаш, Е.В. Метод CRAMM – комплексный подход к оценке рисков [Текст] / Е.В. Гнедаш // Информационные технологии в науке, управлении, социальной сфере и медицине: сборник научных трудов II Международной конференции «Информационные технологии в науке, управлении, социальной сфере и медицине» / под ред. О.Г. Берестневой, О.М. Гергет; Томский политехнический университет. – Томск: Изд-во Томского политехнического университета, 2015. – С. 128-130.

5. Ильинская, Е.В. Методика оценки рисков при разработке автоматизированных информационных систем корпоративного уровня [Текст] / Е.В. Ильинская, В.В. Ломакин, Р.Г. Асадуллаев, Т.В. Зайцева // Научно-технический вестник Поволжья, 2018. – 11. – С. 218-223

6. Файзулаев, Д.Ф. Методы и средства анализа рисков информационной безопасности [Текст] / Д.Ф. Файзулаев // Безопасность информационных технологий, 2017. – Т. 24. – № 3. – С. 69-74.

References

1. Asadullaev, R.G. Development of means for assessing project risks in the creation of information systems for the sphere of public services [Text] / R.G. Asadullaev, V.V. Lomakin, N.P. Putivtseva, O.S. Reznichenko, Yu. Yu. Belokon // Scientific and technical bulletin of the Volga region, 2017. – No. 5. – Pp. 120-122.

2. Vorontsovsky, A.V. Risk Management: Textbook and Workshop for Bachelor's and Master's Degree [Text] / A.V. Vorontsovsky. – Lyubertsy: Yurayt, 2016. – 414 p.

3. Domashchenko, D.V. Risk management in conditions of financial instability [Text] / D.V. Domashchenko, Yu. Finogenova. – M.: Master, INFRA-M, 2010.- 238 p.

4. Gnedash, E.V. CRAMM method – an integrated approach to risk assessment [Text] / E.V. Gnedash // Information technologies in science, management, social sphere and medicine: collection of scientific papers of the II International conference "Information technologies in science, management, social sphere and medicine" / ed. O.G. Berestneva, O.M. Gerget; Tomsk Polytechnic University. – Tomsk: Publishing house of the Tomsk Polytechnic University, 2015. – Pp. 128-130.

5. Ilyinskaya, E.V. Methodology for assessing risks in the development of automated information systems at a corporate level [Text] / E.V. Ilyinskaya, V.V. Lomakin, R.G. Asadullaev, T.V. Zaitseva // Scientific and technical bulletin of the Volga region, 2018. – 11. – Pp. 218-223

6. Fayzulaev, D.F. Methods and tools for the analysis of information security risks [Text] / D.F. Faizulayev // Security of information technologies, 2017. – T. 24. – No. 3. – P. 69-74.

Ильинская Елена Владимировна, кандидат экономических наук, доцент кафедры прикладной информатики и информационных технологий
Скрипина Ирина Ивановна, старший преподаватель кафедры прикладной информатики и информационных технологий

Ilinskaja Elena Vladimirovna, Candidate of Economic Science, Docent of the Department of Applied Informatics and Information Technology
Skripina Irina Ivanovna, Senior Lecturer of the Department of Applied Informatics and Information Technologies

УДК 004.896, 666.9.04 **DOI: 10.18413/2518-1092-2020-5-3-0-7**

Дворянин Д.М.[1]
Загальский А.А.[1,2]
Титов А.И.[3]

СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЯ В МЕНЕДЖМЕНТЕ НА ОСНОВАНИИ ИСТОРИИ КЛИЕНТСКОЙ СЕТИ

[1)] Белгородский государственный национальный исследовательский университет, ул. Победы, д. 85, г. Белгород, 308015, Россия
[2)] Областное государственное автономное учреждение здравоохранения «Детская стоматологическая поликлиника города Белгорода», проспект Славы, д. 58, г. Белгород, 308000, Россия
[3)] Филиал ФКУ "Налог-сервис" ФНС России в Белгородской области, ул. Шершнева, д. 1а, г. Белгород, 308007, Россия

e-mail: 1265279@bsu.edu.ru, titov@bsu.edu.ru

Аннотация
В работе рассмотрен один из основных аспектов формирования системы поддержки принятия решений в менеджменте на основании истории клиентской сети. С помощью технологий структурного моделирования построена модель управления потока заказов в рекламном агентстве. Представлена модель, благодаря которой система определяет статус заказчика. Рассмотрены основные сложности процесса при принятии решений в отношении клиентов. В связи с этим представлена концепция модели интеллектуальной системы, поддерживающей оптимальный выбор заказчиков для их дальнейшего информирования. Упрощает работу менеджера по работе с клиентами, в связи с чем пользователь, работающий с системой, может выполнять больше ключевых задач отличных от работы с клиентами.
Ключевые слова: система поддержки принятия решений; менеджмент; клиентская сеть; история клиентской сети; системно – структурный анализ; управление процессом; интеллектуальная система.

UDC 004.896, 666.9.04

Dvoruanin D.M.[1]
Zagalsky A.A.[1,2]
Titov A.I.[3]

MANAGEMENT DECISION SUPPORT SYSTEM BASED ON THE CLIENT NETWORK HISTORY

[1)] Belgorod State National Research University, 85 Pobedy St., Belgorod, 308015, Russia
[2)] Regional State Autonomous Healthcare Institution "Children's Dental Clinic of the City of Belgorod", 58 Slavy Ave., Belgorod, 308000, Russia
[3)] Branch of fku "Tax-service" of the Federal tax service of Russia in the Belgorod region, Belgorod, 1A Shershneva St., Belgorod, 308007, Russia

e-mail: 1265279@bsu.edu.ru, titov@bsu.edu.ru

Annotation
This paper considers one of the main aspects of forming a decision support system in management based on the history of the client network. Using structural modeling technologies, a model for managing the flow of orders in an advertising Agency was built. The model is also presented, thanks to which the system determines the status of the customer. The main difficulties of the decision-making process in relation to clients are considered. In this regard, the concept of an intelligent system model that supports the optimal choice of customers for their further information is presented. Simplifies the work of the client Manager, so that the user working with the system can perform more key tasks other than working with clients.
Keywords: decision support system; management; client network; client network history; system – structural analysis; process management; intelligent system.

ВВЕДЕНИЕ

В современных реалиях развития информационных технологий ставится вопрос о моделировании систем управления определенными процессами. Начиная от отдельных модулей независимой системы и заканчивая созданием самой системы управления.

При создании таких систем следует начинать с формирования предмета исследования-системы понятий, отражающей существенные характеристики объекта моделирования. Эта задача считается достаточно сложной, что подтверждается различными литературными источниками. Особенностью моделирования сложных систем является универсальность и разнообразие способов его использования, оно становится неотъемлемой частью жизненного цикла системы.

Существует два способа классификации систем: реальные и абстрактные. Выделение систем, состоящих только из технических устройств, почти всегда условно, так как они не способны производить свое состояние. Эти системы действуют как части более крупных, ориентированных на человека организационных и технических систем. Организационная система, для эффективного функционирования которой существенным фактором является способ взаимодействия людей с технической подсистемой, называется человеко-машинной системой [1].

Моделируемая система разработана в соответствии с классификацией, относящейся к абстрактным, так как создана имитационная модель вымышленной компании, предоставляющей рекламные услуги.

ОСНОВНАЯ ЧАСТЬ

Анализ маркетинговых решений поддержки принятия решений в менеджменте

Начальным этапом проектирования данной системы является построение метода стратегического планирования, заключающегося в выявлении факторов внутренней и внешней среды организации и разделении их на четыре категории [2].

В ходе анализа выявлены и проанализированы следующие факторы, такие как сильные и слабые стороны организации, ее возможности и угрозы, которые могут возникнуть в процессе формирования системы, которые представлены в таблице 1

Таблица 1

SWOT-анализ

Table 1

SWOT-analysis

Сильные стороны	Возможности
– Частичное наличие собственного производства – Возможность комплексного обслуживания клиентов – Достаточное техническое оснащение – Сильная профессиональная команда – Минимальные инвестиции и перспективы развития компании	– Возможность расширения ассортимента товаров и услуг – Выгодное географическое положение – Возможность развития рынка – Изменения в рекламных технологиях – Поиск лучших поставщиков
Слабые стороны	**Угрозы**
– Отсутствует четкая организационно-функциональная структура предприятия – Недостаточная квалификация и текучесть кадров – Недостаточный уровень транспортного обеспечения – Отсутствие репутации – Отсутствие постоянных клиентов – Сильная конкуренция	– Колебания цен или демпинг со стороны конкурентов – Появление новых технологий у конкурентов – Снижение деловой активности привело к снижению спроса на услуги – Рост цен на рекламные материалы – Сезонность – Угрозы со стороны контролирующих органов и администрации

Данная таблица построена на основе SWOT-анализа, который проводится на начальном этапе оценки эффективности разработанной системы [3].

Положительными чертами этого анализа являются:

– Универсальность метода, который применим в различных сферах экономики и управления.;

– адаптивность к объекту любого уровня (продукт, предприятие, регион, страна и др.);

– гибкость метода со свободным выбором анализируемых элементов в зависимости от поставленной цели

– может использоваться как для быстрой оценки, так и для долгосрочного стратегического планирования;

– не требует специальных знаний и узкопрофильного образования.

Среди недостатков можно выделить следующие:

– SWOT-анализ показывает только общие факторы. Конкретные меры по достижению этих целей должны разрабатываться отдельно.

– Чаще всего SWOT-анализ только перечисляет факторы без выявления основных и второстепенных, без детального анализа взаимосвязей между ними [4].

– Анализ дает более статичную картину, чем динамическое видение развития.

– Результаты SWOT-анализа обычно представляются в виде качественного описания, в то время как для оценки ситуации часто требуются количественные параметры.

– SWOT-анализ достаточно субъективен и сильно зависит от позиции и знаний человека, который его проводит.

– Для качественного SWOT-анализа необходимо привлекать большие объемы информации из различных областей, что требует значительных усилий и затрат [5].

На основе SWOT-анализа вы можете увидеть описание ситуации, по которой вам нужно принять решение. Выводы, сделанные на основе информации, предоставленной в ходе анализа, следует рассматривать как описание проблемы, поскольку невозможно дать какие-либо рекомендации или установить приоритеты.

Если необходимо получить дополнительную информацию от метода, необходимо сформировать параметры действия на основе пересечения полей. Для этого последовательно рассматриваются различные комбинации факторов внешней среды и внутренних свойств предприятия. Рассматриваются все возможные парные комбинации и выделяются те, которые следует учитывать при разработке стратегии. Пример таблицы поперечного сечения показан на рис. 1.

	Возможности	Угрозы
Сильные стороны	СИВ	СИУ
Слабые стороны	СЛВ	СЛУ

Рис. 1. Таблица поперечного сечения
Fig. 1. Cross-section table

В ходе рассмотрения таблицы поперечного сечения можно выявить следующие закономерности

– Поле СИВ показывает, какие сильные стороны вам нужно использовать, чтобы получить максимальную отдачу от возможностей во внешней среде.

– Поле СЛВ показывает, как внешняя среда может помочь организации преодолеть существующие недостатки.

– Поле СИУ показывает, какие силы необходимо использовать для устранения угроз.

– Поле СЛУ показывает, от каких слабых мест вам нужно избавиться, чтобы попытаться предотвратить надвигающуюся угрозу [6].

Поскольку SWOT-анализ обычно не содержит экономических категорий, он может быть применен к любой организации, отдельному лицу или стране для построения стратегий в самых различных областях.

На основании проведенного анализа можно приступить к формированию СППР.

На рисунках 2-5 представлена контекстная диаграмма системы и ее декомпозиция.

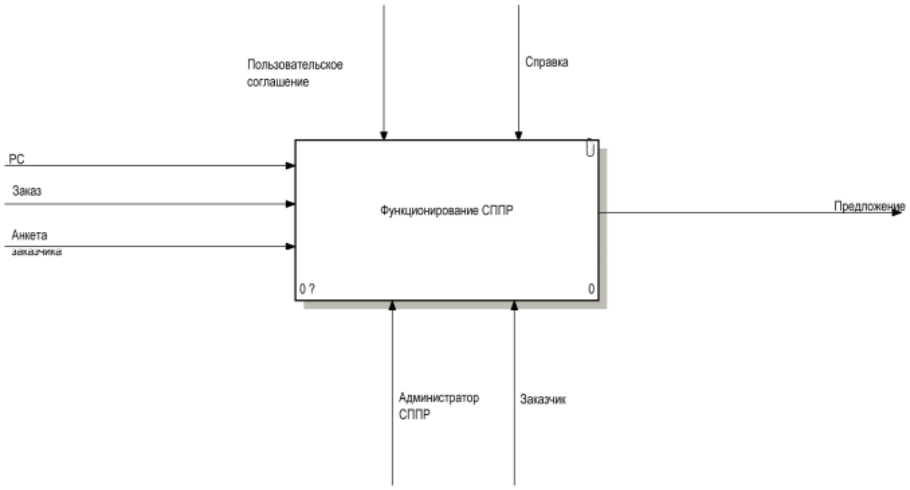

Рис. 2. Контекстная диаграмма Функционирования СППР (IDEF 0)
Fig. 2. Context diagram of the decision support System Functioning (IDEF 0)

На рисунке 3отображена декомпозиция формирования портфеля заказчика исходя из которого можно будет иметь представление по заказчику, сфере его деятельности и предполагаемом будущем заказе [7].

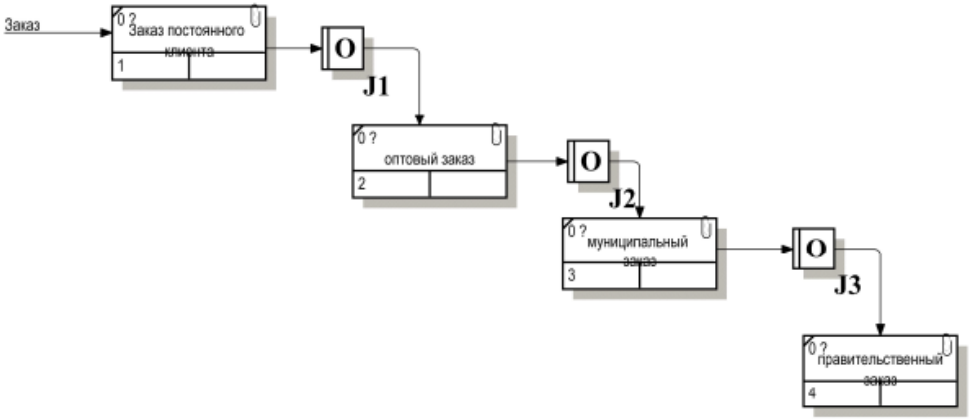

Рис. 3. Декомпозиция Формирования портфеля заказов (IDEF3)
Fig. 3. Decomposition of order portfolio Formation (IDEF3)

На рисунке 4 отображена декомпозиция формирования клиентской сети. В которой система принимает решение кому из заказчиков в имеющейся базе необходимо отправить сообщение о наличии новой продукции, или напомнить о существовании организации вообще [8].

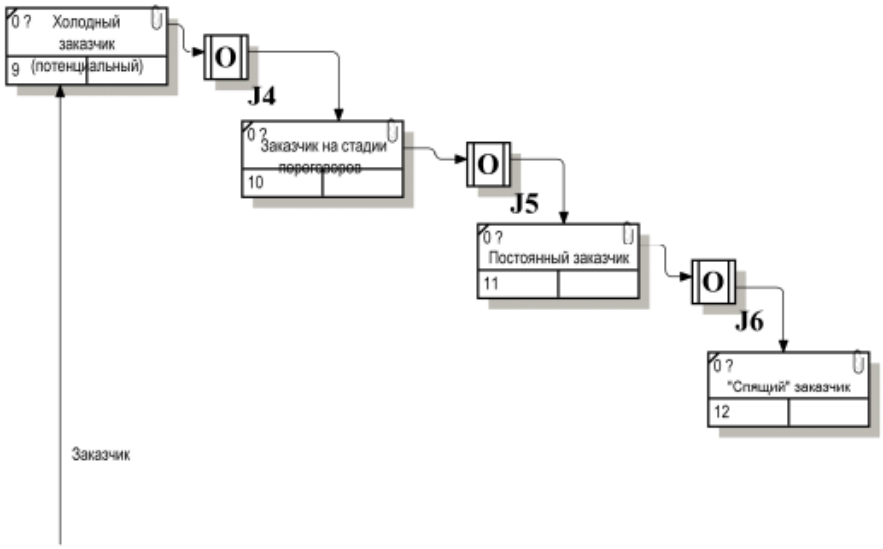

Рис. 4. Декомпозиция формирования клиентской сети (IDEF3)
Pic. 4. Decomposition of the formation of client networks (IDEF3)

Рисунок 5 предполагает собой декомпозицию основного функционала разрабатываемой системы. Благодаря данной декомпозиции можно проследить алгоритм выбора заказчика, которому будет направлено письмо с определенным контекстом [9].

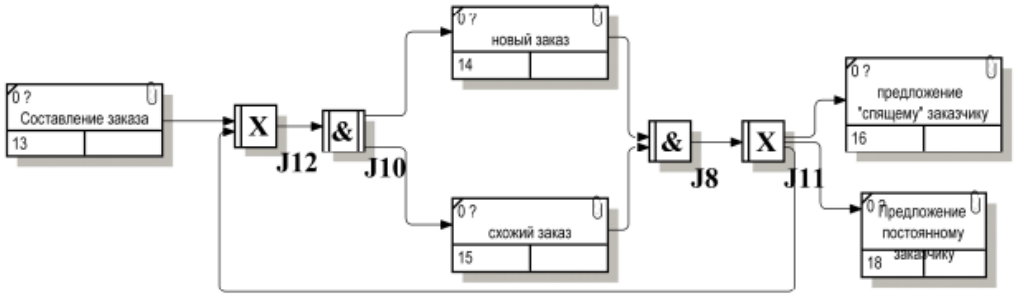

Рис. 5. Декомпозиция Формирования предложения (IDEF3)
Pic. 5. Decomposition of the offer Formation (IDEF3)

ЗАКЛЮЧЕНИЕ

Системы поддержки принятия решений включены в бизнес для поддержки человеческого интеллекта в течение многих лет. Однако эти системы не являются совершенными. Хотя DSSs останавливают лицо, принимающее решение от поощрения предвзятости, они просто помогают в принятии решений, предлагая полезные идеи в отношении легко потребляемых укусов. Идея заключается в том, чтобы представить всю осязаемую информацию в виде графиков, картинок или текста, чтобы вы не упускали из виду факты [10].

Слишком большая зависимость от системы поддержки принятия решений и чрезмерное доверие к ней – это нездоровый признак. С DSS связано много неопределенностей, таких как:

Сложность количественной оценки всех данных: система поддержки принятия решений в основном опирается на поддающиеся количественной оценке данные.

Неосведомленность о допущениях: Принятие решения без учета неконтролируемых факторов может оказаться опасным. Лицо, принимающее решение, должно понимать, что компьютеризированная DSS – это только вспомогательный инструмент.

Отказ конструкции системы: системы поддержки принятия решений конструированы к специфическим потребностям лица, принимающего решение. Такие ситуации могут возникнуть из-за отказа системы проектирования.

Сложность сбора всех необходимых данных: значение, представленное DSS, может быть не 100% верно.

Отсутствие технических знаний у пользователей: хотя системы поддержки принятия решений с годами стали намного проще, многие лица, принимающие решения, по-прежнему испытывают трудности с их использованием. Отсутствие технических знаний остается проблемой.

Список литературы

1. Asefeh Asemi, Ph.D The Role of Management Information System (MIS) and Decision Support System (DSS) for Manager's Decision Making Process / Ph.D Asefeh Asemi. – Iran: International Journal of Business and Management, 2011. – 164-173 с.
2. wisegeek [Электронный ресурс]. – Режим доступа: https://www.wisegeek.com. – Дата доступа: 2020.
3. John, D.O. What is Marketing decision support systems / D.O. John // Article1000.com Knowledge Transfer. – 2017. – № 5. – С. 11
4. managementstudyguide [Электронный ресурс]. – Режим доступа: https://www.managementstudyguide.com. – Дата доступа: 2020.
5. managementstudyhq.com [Электронный ресурс]. – Режим доступа: https://www.managementstudyhq.com. – Дата доступа: 2020.
6. Курейчик В. М. Особенности построения систем поддержки принятия решений //Известия Южного федерального университета. Технические науки. – 2012. – Т. 132. – №. 7.
7. Сокирина А. В., Трифонова О. К. Информационные технологии поддержки принятия решений в рекламной деятельности //Актуальные проблемы авиации и космонавтики. – 2016. – Т. 2. – №. 12.
8. Цебренко К. Н. Системы поддержки принятия решений в современном менеджменте //Альманах мировой науки. – 2016. – №. 2-1. – С. 83-84.
9. Gürel E., Tat M. SWOT analysis: a theoretical review //Journal of International Social Research. – 2017. – Т. 10. – №. 51.
10. Ding J. Advances in network management. – CRC press, 2016.

References

1. Asefeh Asemi, Ph. D The Role of Management Information System (MIS) and Decision Support System (DSS) for Manager's Decision Making Process / Ph. D Asefeh Asemi – Iran: International Journal of Business and Management, 2011. – 164-173 p.
2. wisegeek [Electronic resource]. – Access mode: https://www.wisegeek.com – access date: 2020.
3. John, D. O. What is Marketing decision support systems / D. O. John // Article1000.com Knowledge Transfer. – 2017. – no. 5. – P. 11
4. managementstudyguide [Electronic resource]. – Access mode: https://www.managementstudyguide.com – access date: 2020.
5. managementstudyhq.com [Electronic resource]. – Access mode: https://www.managementstudyhq.com – access date: 2020.
6. Kureychik V. M. features of construction of systems of support of decision-making // Proceedings of the southern Federal University. Technical Sciences, 2012, Issue 132, no. 7.
7. Sokirina A.V., Trifonova O. K. Information technologies for decision support in advertising // Actual problems of aviation and cosmonautics. 2, no. 12.
8. Tsebrenko K. N. decision support systems in modern management // Almanac of world science. – 2016. – №. 2-1. – Pp. 83-84.
9. Gürel E., Tat M. SWOT analysis: a theoretical review // Journal of International Social Research. – 2017. – Т. 10. – №. 51.
10. Ding J. Advances in network management. – CRC press, 2016.

Дворянин Дмитрий Михайлович, магистрант Белгородского государственного национального исследовательского университета»
Загальский Анатолий Анатольевич, системный администратор областного государственного автономного учреждение здравоохранения «Детская стоматологическая поликлиника города Белгорода», магистрант Белгородского государственного национального исследовательского университета»
Титов Алексей Иванович, заместитель директора филиала ФКУ "Налог-сервис" ФНС России в Белгородской области

Dvoryanin Dmitry Mikhailovich, master of «Belgorod State National Research University»
Zagalsky Anatoly Anatolyevich, System Administrator of the Regional State Autonomous Healthcare Institution “Children's Dental Clinic of the City of Belgorod”, Master of the Belgorod State National Research University
Titov Alexey Ivanovich, Deputy Director of the branch of the Federal tax service of Russia In the Belgorod region