DOI 10.37882/2223–2966.2021.10.13

СПОСОБЫ ОБНАРУЖЕНИЯ, БЛОКИРОВКИ И АТРИБУЦИИ ФИШИНГОВЫХ СТРАНИЦ

Назаров Алексей Владимирович
К.воен.н., Военный инновационный технополис «ЭРА», г. Анапа
naazar@mail.ru

Аннотация. На сегодняшний день фишинг — это проблема практически для всех пользователей, бизнеса и сервис-провайдеров по всему миру. Использование фишинга осуществляется для получения конфиденциальной информации. Это могут быть адреса и пароли, банковские реквизиты и другие данные, которые кибермошенники могут использовать для незаконного обогащения, при этом воздействие может осуществляться посредством электронной почты, социальных сетей или телефонной связи.

Фишинг также называют одной из разновидностей социальной инженерии, которая базируется на незнании пользователями основополагающих принципов сетевой безопасности. Кроме того, киберпреступники в своем большинстве оперируют не только технологиями, но и человеческой беспечностью и доверчивостью. Еще в 2011 г. компания Cisco в своем отчете указала на семь основных слабостей человека, которые эксплуатируются преступниками: сексуальность, алчность, тщеславие, чрезмерная доверчивость, лень, сострадание и поспешность в принятии решений.

На сегодняшний день фишинг — это глобальная миллиардная индустрия, ущерб от которой огромен и с каждым годом только возрастает.

В настоящей статье было рассмотрено понятие фишинга, и способы противодействия этому виду мошенничества. Кроме того, приведена статистика ущерба за последние годы с применением этого вида преступлений в информационном поле.

Ключевые слова: фишинг, киберпреступление, информационная безопасность, фишинговые страницы, электронная почта, веб-сайты, мобильный фишинг.

METHODS FOR DETECTING, BLOCKING AND ATTRIBUTING PHISHING PAGES

A. Nazarov

Summary. Today, phishing is a problem for almost all users, businesses, and service providers around the world. Phishing is used to obtain confidential information. These can be addresses and passwords, bank details and other data that cyber fraudsters can use for illegal enrichment, while the influence can be carried out through e-mail, social networks or telephone communications. Phishing is also called a form of social engineering, which is based on users' ignorance of the fundamental principles of network security. In addition, cybercriminals for the most part operate not only with technology, but also with human carelessness and gullibility.

Back in 2011, Cisco identified seven major human weaknesses that are exploited by criminals in a report: sexuality, greed, vanity, gullibility, laziness, compassion, and haste in decision making. Today, phishing is a global billion-dollar industry, the damage from which is enormous and only increases every year. This article discussed the concept of phishing and how to counter this type of fraud. In addition, the statistics of damage in recent years with the use of this type of crime in the information field is presented.

Keywords: phishing, cybercrime, information security, phishing pages, email, websites, mobile phishing.

Термин «фишинг» (phishing) в переводе с английского языка означает «рыбачить», своим происхождением это понятие обязано сходством механизма кибератаки и рыбалки [1].

Злоумышленник выступает со стороны какого-либо известного сервиса и просит ввести пользователя конфиденциальные данные с целью их проверки или обновления. После их введения, преступник получает все, что необходимо для дальнейшего злонамеренного их использования, в большинстве — это получение денежных средств [5].

В настоящее время специалистами фиксируется постоянно возрастающая активность фишинга, нацеленного, как на рядовых пользователей, так и на крупные компании. Проблема усложняется тем, что за последние несколько лет произошло большое количество нарушений данных, в результате чего хакерам стали доступны миллиарды электронных адресов, более того, их можно без проблем приобрести на «черном рынке» в сети интернет [9].

Целью настоящего исследования является анализ ущерба, причиненного киберпретупниками посред-

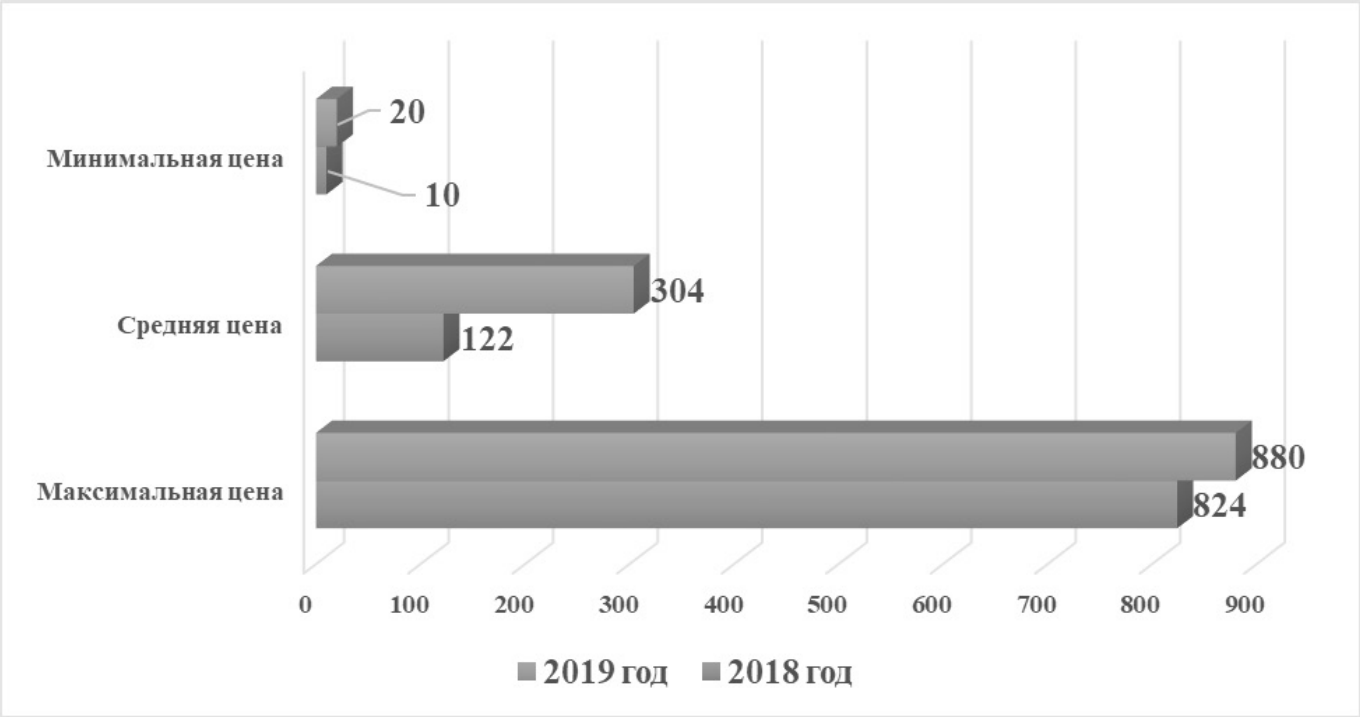

Рис. 1. Динамика цен на фишинг-киты в 2018–2019 гг. в долларах

ством использования фишинга, а также способов обнаружения, блокировки и атрибуции фишинговых страниц. Для реализации цели были определены следующие задачи:

1. дать характеристику понятия фишинг;
2. провести анализ последствий фишинга за последние три года;
3. рассмотреть способы обнаружения, блокировки и атрибуции фишинговых страниц.

Сегодня существует два основных типа фишинга:

- отправка фищингового сообщения, основной целью которого является получение конфиденциальной информации — в данном случае сообщение может передаваться посредством электронной почты или вредоносной программы;
- использование техник целенаправленного фишинга — в качестве примера можно привести: получение информации о высокопоставленных лицах или whaling, создание колонов email-сообщений или clone phishing, принуждение жерты к переводу денежных средств на фальшивый счет в банке или reverse-phishing.

По мнению специалистов, в 2018 г. основными жертвами фишинга являлись физические лица, а самым популярным способом доставки фишинговых писем была электронная почта, соотношение загрузок через веб-браузер и доставки писем по электронной почте составляло 1 к 12. При этом к концу 2018 г. загрузки через веб-браузер сократились до 3%.

Основной тенденцией 2018 г., по мнению специалистов компании CERT-GIB, стало использование публичных сервисов для доставки писем, содержащих вредоносные программы. Сформированный рейтинг включал такие популярные домены, как Россиimail.ru, yandex.ru и gmail.com, это объясняется тем, что преступники старались использовать наиболее доверенные сервисы — те, с которых пользователи привыкли получать электронные письма [11, 12]. Кроме того, это достаточно дешевый способ, поскольку нет необходимости регистрировать новый домен, а в случае обнаружения просто использовать другой почтовый сервис.

На протяжении всего 2018 г. объем фишинга продолжал расти. Так, только в третьем квартале 2018 г. экспертами «Лаборатории Касперского» было обнаружено более половины атак, выявленных за весь 2017 г. Распространению фишинга способствовали: разработка новых схем, заимствование идей по использованию фишинга у иностранных компаний, задействование различных каналов распространения спама и ссылок, эксплуатация популярных тем в качестве приманки.

Так, в соответствии с данными компании Валарм, количество атак на веб-приложения на 2018 г. составляло в среднем 1500 в день. Чемпионат мира по футболу

Рис. 2. Структура распространения фишинга в 2019 г. (по данным на 4 квартал)

в 2018 г. также привлек внимание киберпреступников, которое отразилось в массовой рассылке зараженных файлов под видом расписания игр и турнирной таблицы.

За 2019 г. экспертами компании Group-IB был зафиксирован резкий рост продаж фишинг-китов — конструкторов для массового создания фишинговых сайтов, более, чем в 2 раза [10]. Повышенный спрос на этот популярный инструмент среди мошенников спровоцировал и рост средней цены, которая в результате в 2019 г возросла на 140%. Количество продавцов фишинг-наборов увеличилось на 120%.

Динамика цен на фишинг-киты в 2018–2019 гг. в долларах ($) отражена на рисунке 1.

Эксперты объясняют рост популярности этого инструмента низким порогом при входе на этот рынок и простотой заработка. При этом стоимость набора варьируется в зависимости от его сложности, а конкретно от качества и количества фишинговых страниц.

Фишиннг-кит представляет из себя архивный файл, содержащий скрипты, необходимые для создания фишинг-сайта, которые позволяют мошенникам, не обладающим глубокими знаниями программирования, быстро разворачивать сотни фишинговых страниц, часто страницы используются, как «зеркала» друг друга, при этом, если блокируется один, то активизируется другой.

Для привлечения пользователей, мошенники используют в фишинговых наборах популярные бренды с огромными аудиториями. Так в 2019 г. наиболее часто использовались Amazon, Google, Instagram, Office 365 и PayPal.

Структура распространения фишинга в 2019 г. (по данным на 4 квартал) приведена на рисунке 2.

Так, следуя данным рисунка 2, можно отметить, что в 2019 г. фишинг преимущественно распространялся через веб-сайты, при этом использовались: Spotify, Microsoft, PayPal, Facebook.

Почти треть — 27% принадлежит электронной почте, были использованы такие ресурсы, как Yahoo!, Rbs (Ray-Ban Sunglasses), Microsoft, DropBox.

Через мобильные устройства распространялось 25% фишинга, использовались: Chase Mobile Banking, Facebook, Apple, PayPal. Следует отметить, что через мобильные устройства распространялись преимущественно фишинговые страницы социальных сетей и банков.

Согласно данным Telco Security Trends Report, в этот период телеком-операторы в Европе ежемесячно блокировали в среднем порядка 20 млн. фишинговых атак, при этом было использовано более 7 млн. мобильных

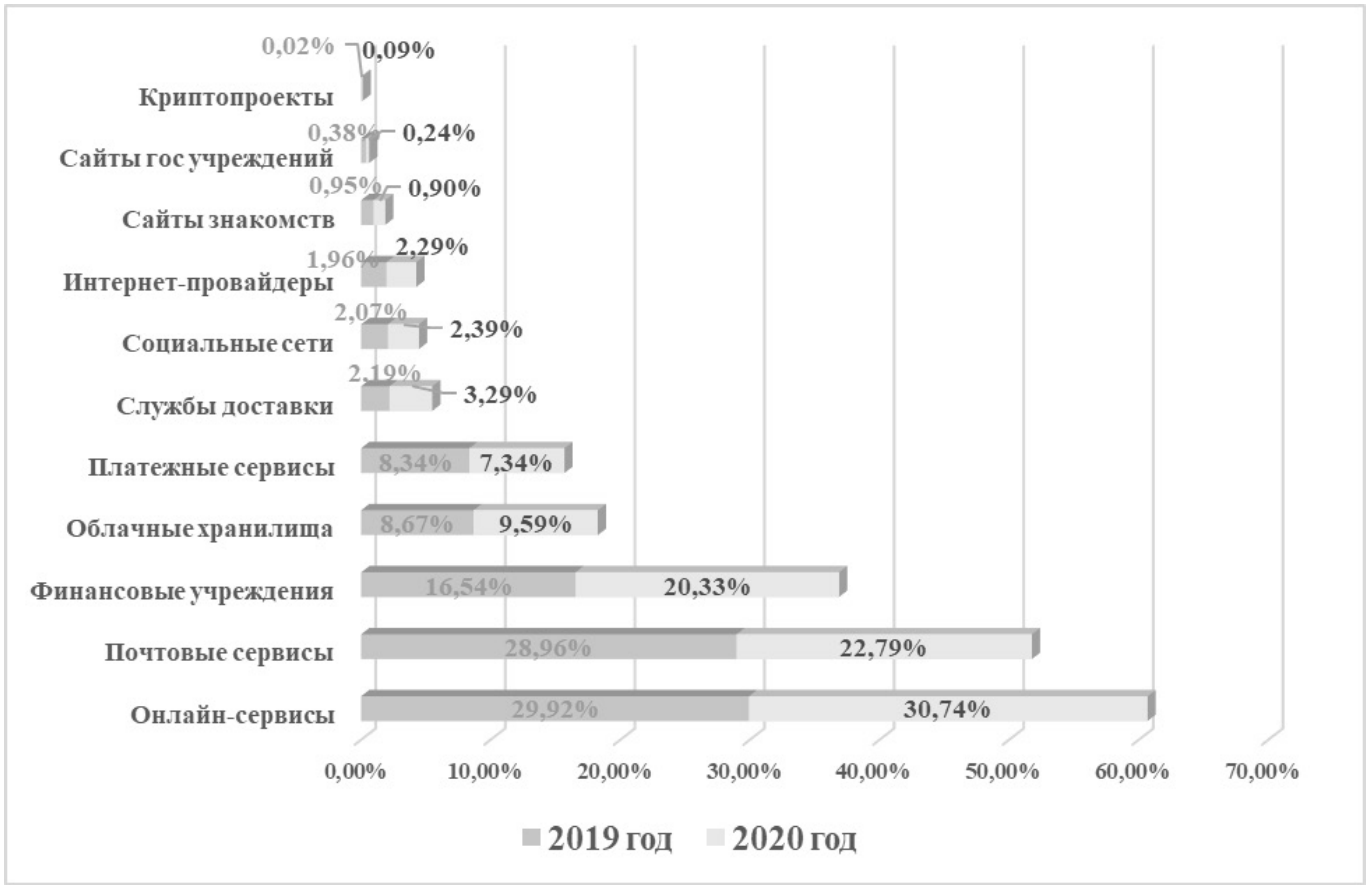

Рис. 3. Структура категорий брендов, используемых чаще всего в фишинг-китах в 2020 г. в сравнении с 2019 г.

абонентов. Также в результате исследования было выявлено, что за этот период мобильный фишинг составил 35% от количества всех активированных блокировок.

По данным ФБР, в 2019 г. фишинг стал самым популярным киберпреступлением, только в США жертвами стали более 114 тыс. человек, причиненный ущерб оценивался в 57,8 млн. долларов [2]. Однако лидером по хостингу фишинговых ресурсов в 2019 г. стала Россия, количество блокировок составило 34%.

В топ-10 инструментов, использовавшихся злоумышленниками в атаках, зафиксированных CERT-GIB в 2019 г., вошли шифровальщик Troldesh (55%); бэкдоры Pony (11%), Formbook (5%), Nanocore (4%) и Netwire (1%); банкеры RTM (6%) и Emotet (5%); и шпионское ПО AgentTesla (3%), Hawkeye (2%), и Azorult (1%). AgentTesla, Netwire и Azorult стали новыми угрозами наблюдаемого периода.

В 2020–2021 гг. согласно отчету Group-IB Hi-Tech Crime Trends было выявлено на 118% больше фишинг-ресурсов, при этом эксперты объясняют это тем, что на фоне сократившихся доходов, легкий заработок привлек внимание большего количества пользователей [4].

Кроме того, в рамках возросших продаж через интернет-каналы, киберпреступники также начали проводить больше фишинговых атак от имени популярных брендов.

Структура категорий брендов, используемых чаще всего в фишинг-китах в 2020 г. в сравнении с 2019 г. представлена на рисунке 3 [6].

Специалисты также отмечают некоторые изменения тактики преступников: если ранее после блокировки хакеры переключались на другие бренды, то в 2020 г. они стали автоматизировать атаки, выводя новые фишинговые единицы на смену заблокированным.

Наибольшее количество фишинга было создано под онлайн-сервисы, их доля в общей структуре составила 39,6%. Также отмечаются почтовые сервисы — 15,6%,

Таблица 1. Количество мобильного фишинга в России за 2020 г.

Вид фишинговой атаки	Количество столкнувшихся с мобильным фишингом,%	Количество пострадавших от мобильного фишинга,%
Электронная почта	52	34
Фишинговые сайты	37	29
Телефонный фишинг	58	37
Смифишинг (фишинг по SMS) [7]	50	31
Физический фишинг	16	13

финансовые учреждения — 15,0%, облачные хранилища — 14,5%, платежные сервисы — 6,6% и т.д. При этом практически исчез фишинг, ориентированный на криптовалютные операции.

В 2020 г. компания Avast проводила опрос российских пользователей, согласно которому 42% россиян сталкивались с фишингом, более того, 27% от него пострадали. При этом две трети опрошенных пострадали, решая личные проблемы, одна треть — при решении рабочих задач.

Кроме того, выросло количество телефонного фишинга, данные за 2020 г. по России представлены в таблице 1.

Эксперты отмечают, что большинство опрошенных пользователей не сообщают о фишинге, их количество составило 61%. Финансовые потери пользователей варьировались от 3,5 тыс. руб. до более 21 тыс. руб.

Несмотря на глобальный охват информационного поля различными видами фишинга, IT-компании не прекращают работу в рамках его обнаружения, блокировки и атрибуции.

Если фишинговая страница обнаружена, существует два пути ее блокировки. Первый, самый распространенный: IT-компания или IT-подразделение передает информацию о странице главным игрокам рынка: производителям браузеров, разработчикам антивирусных решений и хостинг-провайдерам. Эти организации проверяют информацию и принимают решение о блокировке. Минусы данного подхода в том, что за время, требуемое для проверки, появляются новые жертвы мошенников.

Так, за годы своей работы компания Group-IB аккумулировала достаточно обширную базу фишинговых наборов, что позволяет успешно бороться с фишингом, ориентированным на конкретный бренд. При этом база постоянно обновляется и расширяется, как только Group-IB Threat Intelligence обнаруживает новую фишинговую страницу.

Более редкий случай — блокировка по требованию. В некоторых случаях аккредитованные Координационным центром национальных доменов компании могут блокировать фишинговый сайт. В состав таких компаний входят: Group-IB, Лига безопасного интернета, Лаборатория Касперского, RU-CERT, РОЦИТ, Роскомнадзор, Bi. Zone, Банк России и Доктор Веб [8]. Они могут обращаться к регистраторам доменных имен напрямую с требованием прекратить делегирование доменного имени для сайтов, распространяющих фишинг, вредоносное ПО и ботнеты.

Следует отметить, что для повышения эффективности работы IT-компаний необходима автоматизировать их работу, при этом система автоматизация должна включать:

- систему предугадывания места размещения фишинговой страницу;
- систему распознавания фишинга;
- систему автоматического сбора доказательств;
- систему для автоматического реагирования;
- систему обмена индикаторами с производителями браузеров и средств безопасности;
- систему контроля и перепроверки устранения фишинга.

В России противодействием фишингу занимаются антивирусные компании (например, Kaspersky Internet Security, Dr. Web Security Space Pro), которые могут выявлять фишинговые сайты, и внутренние IT-службы безопасности, защищающие свои бренды. Одним из лидеров в этой сфере также является компания Group-IB, которая выводит на рынок антифишинговые решения. Например, такие разработки, как «Система и способ сбора информации для обнаружения фишинга» и «Система и способ обнаружения фишинговых веб-страниц».

Эти разработки анализируют и распознают фишинговый контент по трем составляющим: по текстовому содержимому страницы, по блоку данных (текст и изображение) и по изображениям на странице (три запатентованных компанией Group-IB подхода).

Особой проблемой в блокировке фишинга является предварительное предугадывание места его появления, компания Group-IB имеет такую технологию.

Анализ основан на двух подходах атрибуции: патерны (характеристики) поведения и корреляция на накопленной базе данных известных фишинговых сайтов, созданных одними и теми же группами мошенников (они имеют определенные общие признаки).

Когда характеристики выделены, технология позволяет предсказать, на каких новых серверах будет активирован вредоносный контент. Для этого используется система создания снимков сети интернет, которые связаны между собой. Далее эти снимки накладываются друг на друга. В результате сравнения определяются условные 10 серверов из 2 млрд. хостов, на которых могут появиться фишинг-группы, а также пути, по которым они будут размещаться.

Относительной новыми инструментами в борьбе с фишингом являются аватары в интернет-банках или корпоративных магазинах. В процессе захода на сайт картинка подгружается на сайт с компьютера пользователя, если пользователь заходит на поддельный сайт, то аватарка будет другая.

Однако, по мнению специалистов наиболее эффективным способом борьбы с фишингом является искусственный интеллект. Подобные сервисы анализируют инфраструктуру злоумышленников, предугадывают создание новых фишинговых доменов и сообщают об этом пользователю.

В доработанной версии паспорта федерального проекта «Информационная безопасность» говорится, что уже в 2021 г. будет разработана платформа для мониторинга фишинговых (мошеннических) сайтов и утечек персональных данных. На ее создание потратят 1,4 миллиарда рублей [3].

Таким образом, фишинг является серьезной проблемой для огромного количества пользователей в интернет-пространстве. В этой связи разработка новых инструментов, позволяющих обнаруживать и блокировать фишинговые страницы является актуальной. Рассмотренные способы борьбы с фишингом позволят снизить эффективность использования фишинга злоумышленниками.

ЛИТЕРАТУРА

1. Атака клонов: чем опасны фишинговые сайты. Фишинг образца 2020 года: как трансформировались фейки и как от них защититься / [Электронный ресурс] URL: https://www.kommersant.ru/conference/735
2. Ломают без взлома: фишинг стал еще опаснее / [Электронный ресурс] URL: https://www.gazeta.ru/tech/2020/07/20/13159111/phishing_danger.shtml
3. На борьбу с фишингом потратят 1,4 миллиарда рублей / [Электронный ресурс] URL: https://newizv.ru/news/society/30–09–2020/na-borbu-s-fishingom-potratyat-1–4-milliarda-rubley
4. Оборот не туда: число фишинг-ресурсов в 2020 г. выросло на 118% / [Электронный ресурс] URL: https://iz.ru/1091824/natalia-ilina/oborot-ne-tuda-chislo-fishing-resursov-v-2020-godu-vyroslo-na-118
5. Обучен, значит вооружен: самые опасные случаи фишинга в 2020 году / [Электронный ресурс] URL: https://hightech.plus/2020/10/02/obuchen-znachit-vooruzhen-samie-opasnie-sluchai-fishinga-v-2020-godu
6. Фишинг в 2020 г. / [Электронный ресурс] URL: https://ict.moscow/research/fishing-v-2020-godu/
7. Число выявленных и заблокированных фишинг-ресурсов выросло на 118% / [Электронный ресурс] URL: https://news.myseldon.com/ru/news/index/239901709
8. Эксперты выявили резкий рост числа фишинговых сайтов в мире / [Электронный ресурс] URL: https://ria.ru/20201019/fishing-1580414537.html
9. «Это срочно»: число жертв интернет-фишинга выросло в десятки раз / [Электронный ресурс] URL: https://www.rbc.ru/spb_sz/07/09/2020/5f55fb159a7947398ef9a335
10. 2019 установил рекорд по числу блокировок фишинговых ресурсов / [Электронный ресурс] URL: https://www.comnews.ru/content/207038/2020–05–08/2020-w19/2019-ustanovil-rekord-chislu-blokirovok-fishingovykh-resursov
11. [Электронный ресурс] URL: https://scholar.google.com.tw/citations?view_op=view_citation&hl=ru&user=Xc6gkP8AAAAJ&citation_for_view=Xc6gkP8AAAAJ: u-x6o8ySG0sC (дата обращения: 30.09.2021).
12. [Электронный ресурс] URL: http://publishing-vak.ru/file/archive-economy-2021–5/14-cozac.pdf (дата обращения: 30.09.2021).

Журнал «Современная наука: актуальные проблемы теории и практики»