

Мария Михайловна Акулич

*доктор социологических наук, профессор кафедры общей и экономической социологии
Тюменского государственного университета, г. Тюмень, m.m.akulich@utmn.ru*

Гбенга Олалекан Олову

*аспирант кафедры общей и экономической социологии Тюменского государственного
университета, г. Тюмень, gbengahollowu@gmail.com*

ОЦЕНКА ВЛИЯНИЯ КИБЕРБЕЗОПАСНОСТИ НА ЭЛЕКТРОННЫЙ БАНКИНГ В НИГЕРИИ

Аннотация. Основная цель статьи — оценить влияние кибербезопасности на электронный банкинг в Нигерии. Интернет, без сомнения, является частью человеческого существования. Вся деятельность человека во всех фазах жизни либо уже в Интернете, либо почти в Интернете. Среди многочисленных секторов, в которые хорошо интегрирован Интернет, входит банковский сектор. Многие ученые исследовали электронный банкинг; плюсы и минусы, другие объяснили важность передовой системы кибербезопасности для банковских услуг. Тем не менее, среди множества социологических исследований, проведенных либо в области кибербезопасности, либо в области электронных банковских операций, очень мало научных работ, в которых дается оценка кибербезопасности электронных банковских операций в Нигерии. Таким образом, это исследование направлено на изучение уровня безопасности или нарушений кибербезопасности как фактора, оказывающего значительное влияние на электронный банкинг в Нигерии. В исследовании использовались как количественные, так и качественные методы исследования. Для обсуждения использовались вторичные данные из надежных открытых источников и ученых. Исследование показало, что в банковской системе Нигерии были нарушения из разных областей. Сделан вывод, что оценка уровня кибербезопасности является низкой по сравнению с тем, что ожидается, чтобы избежать многочисленных прогнозируемых атак в киберпространстве в ближайшие годы.

Ключевые слова: кибербезопасность, электронный банкинг, интернет-банкинг, киберпространство.

Maria Mikhailovna Akulich

*Doctor of Sociology, Professor, Department of General and Economic Sociology
at Tyumen State University, Tyumen, m.m.akulich@utmn.ru*

Gbenga Adelekan Olovu

*Postgraduate student, Department of General and Economic Sociology
at Tyumen State University, Tyumen, gbengahollowu@gmail.com*

ASSESSMENT OF THE IMPACT CYBERSECURITY ON ELECTRONIC BANKING IN NIGERIA

Abstract. The main aim of the article is to assess the impact of cybersecurity on electronic banking in Nigeria. The internet is no doubt part of human existence. All activities of man in all phases of life are either already on the internet or almost on the internet. Among the numerous sectors that the internet has been well integrated is the banking sector. Many scholars have investigated electronic banking; pros and cons, others have explained the importance of advanced cybersecurity system for banking services. Nevertheless, among the plethora of sociological research that has been carried out on either cybersecurity or electronic banking, there is a paucity of scholarly work that provides an assessment of cybersecurity on electronic banking in Nigeria. This study is therefore aimed at investigating the cybersecurity safety level or breaches as a factor with significant impact on electronic banking in Nigeria. The study made use of both quantitative and qualitative research methods. Secondary data from reliable open sources and scholars were used for discussion. The research discovered that there has been breaches in Nigeria banking system from different areas. It was therefore concluded that the cybersecurity level assessment is low compared to what is expected to have in order avoid the numerous predicted attacks in the cyber space years to come.

Keywords: cybersecurity, electronic banking, internet banking, cyber space.

Кибербезопасность в настоящее время изучается многими российскими и зарубежными исследователями, среди которых Ю. А. Караева, Н. Ю. Сайбель [1], П. В. Ревенков, А. А/ Бердюгин, [2], Н. В. Рачева, Ф. В. Балеевских, В. В. Котов [3], Н. Н. Мартыненко, А. В. Овчаренко [4], А. А. Салкуцан, Р. Т. Ниязов [5] и др.

Электронный банкинг (e-banking) является определенным свидетельством важности Интернета в нашем современном мире. Безналичная политика, принятая во всем мире, является одним из основных факторов, вызвавших появление электронного банкинга. Ожидается, что электронный банкинг поможет сократить контакты с банковским залом, персоналом и наличными. Нигерия как и другие страны стремится к достижению этой цели. «В рамках нашего стремления стать одной из 20 лучших экономик до 2020 г., CBN проинформировал мир о том, что Нигерия начнет процесс перехода к безналичной экономике к январю 2012 г., уменьшив количество банкнот и монет найры (наличных денег), используемых для бизнеса, но не отказавшись от использования наличных денег [6]. Эти намерения не только не реализованы к 2020 г., но и до настоящего времени во многом остаются пожеланиями. Причина этого объективная, поскольку безналичная политика не может быть достигнута в одном секторе экономики. Она нуждается в адекватной ориентации на использование системы электронного банкинга. Это предполагает возможность клиента переводить деньги в электронном виде через любое банковское приложение со смартфона или компьютера. Это также включает в себя способность человека оплачивать товары или услуги с помощью карты банкомата.

С помощью Интернета электронный банкинг помогает клиенту напрямую общаться со своим менеджером по работе с клиентами через чат или по почте. Печать выписки со счета становится проще. Глядя на удобства, которые может предложить электронный банкинг; следует задаться вопросом, почему все население Нигерии еще не использует электронный банкинг [7]. Статистические данные и результаты ранее проведенных исследований показывают, что это во многом связано с проблемой безопасности. В этой связи, предметом нашего исследования является изучение фактора безопасности и его влияния на развитие электронного банкинга в Нигерии. Важно отметить, что в целом банковская система может обеспечить безопасность клиентов с помощью адекватной системы кибербезопасности. Однако важно знать мнение населения, о проблемах в той сфере и оценку кибербезопасности электронных банковских операций населением Нигерии.

Исследование направлено на изучение кибербезопасности в банковской системе Нигерии с использованием информации о взломе банковской системы, и оценке влияния кибербезопасности на электронный банкинг в Нигерии для анализа готовности к прогнозируемым кибератакам.

При проведении исследования были использованы качественные и количественные методы исследования. В качественном методе использовались метод контент анализа, а также анализ научных материалов по рассматриваемой теме и соответствующих организационных отчетов, размещенных в интернете в открытом доступе. В количественном методе использовались надежные вторичные данные из открытых источников или государственных организаций, имеющих отношение к данному исследованию. Полученные данные описаны и проанализированы.

Далее представлены результаты исследований.

Нарушения кибербезопасности в Нигерии

В общем, нарушение безопасности — это любой инцидент, который приводит к несанкционированному доступу к компьютерным данным, приложениям, сетям или устройствам. Это приводит к доступу к информации без авторизации. Как правило, это происходит, когда злоумышленнику удается обойти механизмы безопасности [8]. Национальный институт стандартов и технологий, NIST, Министерство торговли США определили нарушение концепции кибербезопасности как «Потеря контроля, компрометация, несанкционированное раскрытие, несанкционированное приобретение или любое подобное событие, когда: лицо, не являющееся авторизованным пользователем, получает или потенциально может получить доступ к информации, позволяющей установить личность; или авторизованный пользователь получает доступ к информации, позволяющей установить личность, для иной, чем авторизованная, цели» [9].

Таким образом, нарушение кибербезопасности можно охарактеризовать как несанкционированный доступ к другой отдельной электронной информации через пользователя компьютера и Интернета в любых личных целях, которые могут включать использование личности жертвы, сбор выкупа за информацию, подлежащую возврату, продажу информации для товарищей-хакеров, чтобы купить для клонирования, или просто сделать его доступным для обществу.

По данным компании Sophos, специализирующейся на кибербезопасности, в своем отчете за 2022 г. Нигерия заняла 11-е место среди стран, подвергшихся атакам ransomware. На рис. 1 представлен этот отчет в виде графика.

Процент организаций, пораженных программами-вымогателями за последний год

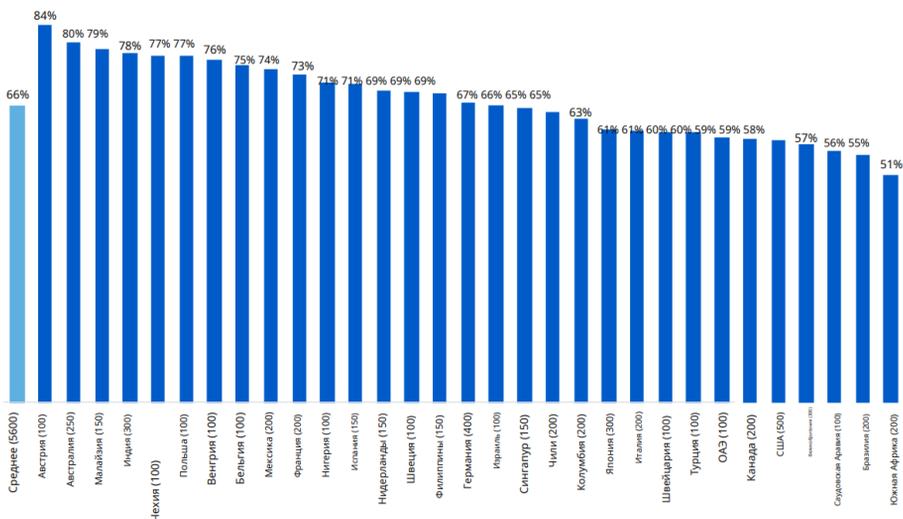


Рис. 1. Страны с наибольшим количеством организаций, пострадавших от ransomware в 2022 г.

Источники: [10].

Положение Нигерии под номером 11 подтверждается некоторыми другими исследованиями, проведенными различными организациями и учеными. Высока вероятность того, что часть организаций, пострадавших в Нигерии в 2022 г., относится к банковскому сектору.

Банковская система Нигерии подверглась многочисленным нарушениям кибербезопасности. Согласно исследованиям, проведенным Augusto&Co, 2022. 59% клиентов банка заявили, что стали жертвами мошенничества с интернет-банкингом. При этом 41% отметили, что они не были скомпрометированы. Пострадавших был распределены в соответствии с тремя основными способами компрометации: фишинг, взлом данных и несанкционированный доступ к аккаунту через Неструктурированные дополнительные служебные данные, USSD [11].

Фишинг, кража личных данных, онлайн-мошенничество, хакерство и ransomware — вот некоторые популярные формы атак на жертв в киберпространстве [12, 13, 14]. С другой стороны, Виктория и др., 2022, определили три основных нарушения кибербезопасности, включая вирусы, черви и трояны, рассылку спама по электронной почте и киберпреследование. На рис. 2 показаны нарушения, с которыми столкнулась банковская система Нигерии.

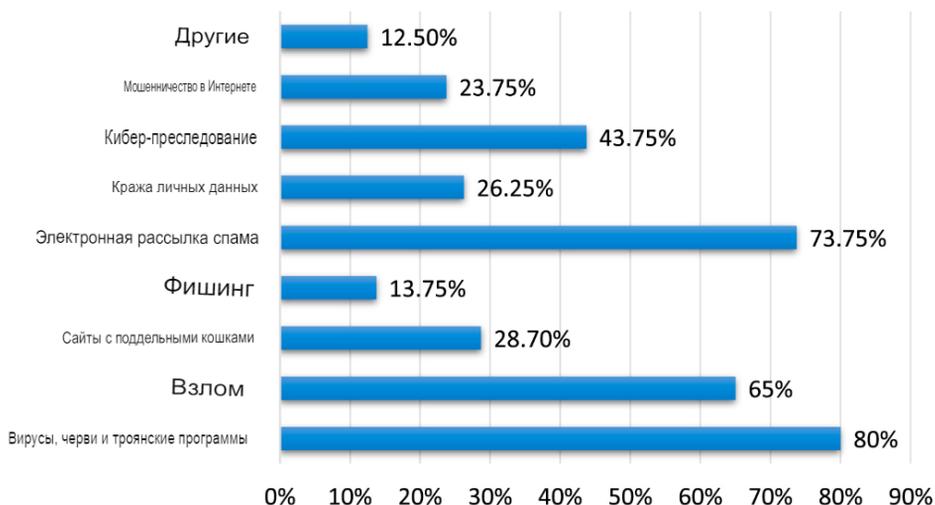


Рис. 2. Электронный опыт нарушений кибербезопасности в банковской отрасли Нигерии

Источник: [7].

Предотвращение потенциальных кибератак в будущем

По данным, приведенным Годфри Джорджем в 2018 г. коммерческий банк потерял в совокупности 15 млрд долларов (39 миллионов долларов) из-за электронного мошенничества, что на 55% больше, чем в предыдущие годы. В период с июля по сентябрь 2020 г. банки, по данным Нигерийской системы межбанковских расчетов, потеряли 3,5 млрд найр в результате инцидентов, связанных с мошенничеством, что на 534% больше, чем за тот же период 2019 г., когда этот показатель составлял 552 млн найр [13].

Кибератаки в Нигерии не ограничиваются банковским сектором, а получили широкое развитие и в других секторах, сотрудники пользователи которых столкнулись с проблемой кибератак. Это академические секторы (университеты) и государственные полугосударственные предприятия. В ходе анализа и прогнозирования кибербезопасности на 2023 год, рассмотренных Deloitte в статье «Перспективы кибербезопасности в Нигерии на 2023 год», ожидалось, что выборы 2023 г. в Нигерии подвергнутся атаке злоумышленника [14]. Это ожидание, как выяснилось, в конечном счете произошло. Министр связи и цифровой экономики Иса Пантиами отметил: «Во время президентских выборов 2023 г. было совершено 12,9 млн (12 988 978) кибератак как внутри, так и за пределами Нигерии» [15].

В Нигерии проводится работа по профилактике и предотвращению кибератак. Так, банковский сектор Нигерии неоднократно проводил тренинги для своего ИТ-персонала, но статистика показывает, что это оказалось пока малоэффективным. Борьба с киберпреступниками должна продолжаться. Чем больше решений по кибербезопасности предоставляется, тем чаще киберпреступники используют новую тактику, чтобы превзойти защиту инноваций клиентов. Согласно заключению Нигерийской системы межбанковских расчетов, NIBSS, «все больше нигерийцев совершают электронные транзакции ежедневно, так же, как и всплеск киберпреступлений, поскольку киберпреступники становятся все более искусными в чистке банковских счетов ничего не подозревающих пользователей [16].

Глядя на рост числа киберпреступлений в Нигерии из года в год, нетрудно предсказать, что в ближайшие годы существует вероятность роста. Нигерийская Инициатива по информированию потребителей и финансовому просвещению (SAFEi) прогнозирует к 2030 г. убытки от киберпреступлений в Нигерии и за ее пределами в размере 6 триллионов долларов. Эти преступления совершаются в основном посредством фишинга и кражи личных данных [17].

В Нигерии, как и в любой другой стране, нет проблем с определением вероятного увеличения числа кибератак до того, как они произошли. Проблема в том, как часто вносятся надлежащие исправления, достаточны ли они для того, чтобы скорректировать ожидания, избежать или, по крайней мере, снизить уровень риска? Существует четыре индикатора кибербезопасности: обучение банковского персонала, использование современных технологий, поддержка руководства банка по вопросам кибербезопасности и приоритизация вопросов кибербезопасности. Согласно полученным данным, только «поддержание современных технологий» составляет 40%, у других — 60% и выше [7].

При этом вопрос не только в обучении персонала и проявлении заботы со стороны руководства банка, а главным образом в используемых банком технологиях. Кроме того, необходимо отметить, что борьба с кибербезопасностью предназначена не только для организации или правительства. Клиенты должны заботиться о том, чтобы не стать жертвами киберпреступников. Об этом свидетельствует доклад, представленный «Лабораторией Касперского», российским многонациональным поставщиком антивирусных и кибербезопасных услуг (18.). А. Адепету Адейеми отмечает, что «малые и средние предприятия (МСП) в Нигерии сталкиваются с большим количеством киберугроз, при этом число

атак увеличилось на 89% в прошлом году. По данным исследователей «Лаборатории Касперского» и других авторов, оценивших динамику атак на МСП в период с января по апрель 2022 г. и за тот же период 2021 г. отмечено, что эти угрозы представляют растущую опасность для предпринимателей» [18].

В заключении отметим, что банковский сектор Нигерии уязвим для кибератак. Уязвимость возрастает по мере того, как все больше людей принимают государственную политику безналичных расчетов, которая может быть достигнута только с использованием системы электронного банкинга. Научно-исследовательские институты, ученые, компании, занимающиеся кибербезопасностью, и государственные учреждения регулярно сообщают о нарушениях кибербезопасности. Проведенное нами исследование позволяет сделать вывод о том, что проблема кибербезопасности в Нигерии все больше актуализируется, а приемы нарушения кибербезопасности становятся все более изощренными благодаря появлению и использованию новых технологий. Киберпреступники намного опережают нигерийских экспертов по кибербезопасности. Существует значительная нехватка передовых технологий для предотвращения угроз кибербезопасности и реагирования на нарушения кибербезопасности после их обнаружения. Важно и необходимо также повышать компьютерную и финансовую грамотность населения, пользователей банковских услуг. Совместные усилия банковских учреждений и клиентов могут оказать значительное влияние на повышение уровня кибербезопасности в системе электронного банкинга.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Караева Ю. А. Кибербезопасность в системе интернет-банкинга / Ю.А. Караева, Н.Ю. Сайбель // Международный журнал гуманитарных и естественных наук. — 2021. — № 2-1. // Научная электронная библиотека «КиберЛенинка»: сайт. — URL: <https://cyberleninka.ru/article/n/kiberbezopasnost-v-sisteme-internet-bankinga> (дата обращения: 10.04.2023).
2. Ревенков П.В. Социальная инженерия как источник рисков в условиях дистанционного банковского обслуживания / П.В. Ревенков, А.А. Бердюгин // Национальные интересы: приоритеты и безопасность. — 2017. — № 9 (354). Научная электронная библиотека «КиберЛенинка»: сайт. — URL: <https://cyberleninka.ru/article/n/sotsialnaya-inzheneriya-kak-istochnik-riskov-v-usloviyah-distantsionnogo-bankovskogo-obsluzhivaniya> (дата обращения: 10.04.2023).
3. Рачева Н.В. Современные способы совершения мошенничества в отношении имущества физических лиц с использованием интернет-ресурсов и технологий социальной инженерии / Н.В. Рачева, Ф.В. Балеевских, В.В. Котов // Юридическая наука. — 2021. — № 2. // Научная электронная библиотека «КиберЛенинка»: сайт. — URL: <https://cyberleninka.ru/article/n/sovremennye-sposoby-soversheniya-moshennichestva-v-otnoshenii-imuschestva-fizicheskikh-lits-s-ispolzovaniem-internet-resursov-i> (дата обращения: 10.04.2023).
4. Мартыненко Н.Н. Мошенничество в сфере дистанционного банковского обслуживания и методы борьбы с ним в условиях пандемии / Н.Н. Мартыненко, А.В. Овчаренко // Инновации и инвестиции. — 2020. — № 12 // Научная электронная библиотека «КиберЛенинка»: сайт. — URL: <https://cyberleninka.ru/article/n/moshennichestvo-v-sfere-distantsionnogo-bankovskogo-obsluzhivaniya-i-metody-borby-s-nim-v-usloviyah-pandemii> (дата обращения: 10.04.2023).

5. Салкуцан А.А. Анализ современных уязвимостей информационной безопасности финансовых приложений российских банков / А.А. Салкуцан, Р.Т. Ниязов // Экономический журнал. — 2020. — № 2 (58). // Научная электронная библиотека «КиберЛенинка»: сайт. — URL: <https://cyberleninka.ru/article/n/analiz-sovremennyh-uyazvimostey-informatsionnoy-bezopasnosti-finansovyh-prilozheniy-rossiyskih-bankov> (дата обращения: 10.04.2023).
6. Cashless policy in Nigeria // Website of the Central Bank of Nigeria [website]. — URL: <https://www.cbn.gov.ng/cashless/Cash-Less%20FAQs.pdf/> (дата обращения: 04.04.2023).
7. Victoria W. Internet banking in Nigeria: cybersecurity violations, practices and opportunities / Victoria W. [et al.] // International Journal of Legal Crime and Justice. — 2020, URL: <https://doi.org/10.1016/j.ijlcj.2020.100415>(дата обращения: 04.04.2023).
8. Что такое нарушение безопасности? // Лаборатории Касперского [сайт]. — URL: <https://www.kaspersky.com/resource-center/threats/what-is-a-security-breach> (дата обращения: 04.04.2023).
9. Security and Privacy Controls for Information Systems and Organizations // National Institute of Standards and Technologies, NIST [website]. — URL: <https://csrc.nist.gov/glossary/term/breach#:~:text=The%20loss%20of%20control%2C%20compromise,information%20for%20another%20than%20authorized/> (дата обращения 04.04.2023).
10. The State of Ransomware // Sophos official website [website]. — URL: <https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf/> (дата обращения: 02.04.2023).
11. 2022 Consumer Digital Banking Satisfaction Index // Official website of Augusto&co Rating Agency [website]. — URL: <https://www.agusto.com/2022-consumer-digital-banking-satisfaction-index/> (дата обращения: 02.04.2023).
12. Gbenga Olowu, Cybercrime in Nigeria: Evolution and forms // International Scientific Conference [website]. — URL: https://www.academia.edu/97442557/Cyber-crime_in_Nigeria_Evolution_and_forms/ (дата обращения: 02.04.2023).
13. Godfrey George, Bank customers, companies lose billions to Nigeria's weak cybersecurity // Punch Newspaper [website]. — URL: <https://punchng.com/bank-customers-companies-lose-billions-to-nigerias-weak-cybersecurity/?amp> (дата обращения 04.04.2023).
14. Nigeria cyber security outlook // Deloitte [website]. — URL: <https://www2.deloitte.com/za/en/nigeria/pages/risk/articles/nigeria-cybersecurity-outlook-2023.html> (дата обращения: 04.04.2023).
15. Mary Izuaka, Nigeria recorded 12.9 million Cyber attacks during presidential // Premium Time Newspaper. — URL: <https://www.premiumtimesng.com/business/business-news/587712-nigeria-recorded-12-9-million-cyber-attacks-during-presidential-nass-elections-minister.html/> (дата обращения 04.04.2023).
16. Adeyemi Adepetun, Cybercrimes raise concerns for N30.2tr monthly e-payments // The Guardian Newspaper. — URL: <https://guardian.ng/news/cybercrimes-raise-concerns-for-n30-2tr-monthly-e-payments/> (дата обращения: 04.04.2023).
17. Maurice O. Cybercrime in Nigeria requires actions of the public and private sectors // Institute for Security Studies. — URL: <https://issafrica.org/iss-today/cybercrime-in-nigeria-demands-public-private-action/> (дата обращения: 04.04.2023).
18. Adeyemi Adepetun, Cyber attack on Nigerian SMEs up by 89 per cent in 2022 // The Guardian Newspaper. — URL: <https://guardian.ng/business-services/cyber-attack-on-nigerian-smes-up-by-89-percent-in-2022/> (дата обращения 04.04.2023).