ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/2587-5671-2021-25-6-212-226
УДК 336:004.056(045)
JEL G21, G32, L86

Фишинговые схемы в банковской сфере: рекомендации пользователям интернета по защите и разработка задач регулирования

П.В. Ревенков[a] ✉, **К.Р. Ошманкевич**[b], **А.А. Бердюгин**[c]
[a, c] Финансовый университет, Москва, Россия;
[b] Московский государственный лингвистический университет, Москва, Россия
[a] https://orcid.org/0000-0002-0354-0665; [b] https://orcid.org/0000-0003-3539-003X;
[c] https://orcid.org/0000-0003-2301-1776
✉ Автор для корреспонденции

АННОТАЦИЯ

Цель и задачи исследования заключаются в анализе мошеннических фишинговых схем, разработке рекомендаций пользователям интернета и соответствующих задач регулирования. **Актуальность** темы статьи обусловлена особенностями работы в киберпространстве с возникновением новых источников банковских рисков как для клиентов, так и для самих организаций. **Научная новизна** рукописи заключается в подробном анализе фишинговых схем, разработке рекомендаций и направлений применительно к Российской Федерации. **Объект** исследования — кибермошенничество в кредитно-финансовой сфере; **предмет** — социальная инженерия и фишинговые схемы. **Методология** статьи включает системный анализ литературы и источников по теме исследования, общенаучные методы (анализ, синтез, дедукция, аналогия, классификация), корреляционный анализ данных, графическую визуализацию информации. Авторы рассматривают основные методы фишинга и наиболее распространенные приемы, которые используют кибермошенники. Проведен критический анализ литературы, который позволил определить перспективное направление для научно-технического потенциала России. Выполнен корреляционный анализ связи количества киберпреступлений и коммерческих банков. Даны **рекомендации** для пользователей интернета (как распознать признаки мошенничества), а также для регулирующих органов по совершенствованию системы надзора за распространением информации в киберпространстве. Сделан **вывод** о необходимости повышения уровня киберграмотности и общей грамотности населения, с одной стороны, и модернизации способов осуществления надзора и контроля за информацией, размещаемой в сети Интернет, с другой стороны, для эффективного противодействия финансовой и киберпреступности. Полученные **результаты** могут быть использованы при дальнейшем развитии дистанционных банковских услуг, оказываемых населению, в целях повышения конкурентоспособности на рынке банковских услуг. **Перспективы** дальнейшего исследования данной темы состоят в расширении ее структуры, развитии компетенций специалистов в области технологий дистанционного банковского обслуживания, а также развитии научно-технического потенциала России.

Ключевые слова: киберпространство; фишинг; кибербезопасность; киберграмотность; дистанционное банковское обслуживание; риски; злоумышленник; пользователь; фиктивная организация

Для цитирования: **Ревенков П.В., Ошманкевич К.Р., Бердюгин А.А. Фишинговые схемы в банковской сфере: рекомендации пользователям интернета по защите и разработка задач регулирования. *Финансы: теория и практика.* 2021;25(6):212-226. DOI: 10.26794/2587-5671-2021-25-6-212-226**

ORIGINAL PAPER

Phishing Schemes in the Banking Sector: Recommendations to Internet Users on Protection and Development of Regulatory Tasks

P.V. Revenkov[a] ✉, **K.R. Oshmankevich**[b], **A.A. Berdyugin**[c]
[a, c] Financial University, Moscow, Russia; [b] Moscow State Linguistic University, Moscow, Russia
[a] https://orcid.org/0000-0002-0354-0665; [b] https://orcid.org/0000-0003-3539-003X;
[c] https://orcid.org/0000-0003-2301-1776
✉ Corresponding author

ABSTRACT

The **aim and objectives** of the article are to analyze fraudulent phishing schemes and develop recommendations for Internet use and relevant regulatory tasks. The **relevance** of the article is due to the peculiarities of working in cyberspace with the emergence of new sources of banking risks, both for customers and organizations. The **scientific novelty** of the manuscript consists of a detailed analysis of phishing schemes, the development of recommendations and directions in relation to the Russian Federation. The **object** of the study is cyber fraud in the credit and financial sphere; the **subject** is social engineering and phishing schemes. The **methodology** of the paper includes a systematic analysis of the literature and sources on the research topic, general scientific methods (analysis, synthesis, deduction, analogy, classification), correlation analysis of data, graphical visualization of information. The authors **consider** the main methods of phishing and the most common techniques used by cybercriminals. Based on the critical analysis of the literature the authors determined a promising direction for the scientific and technical potential of Russia. A correlation analysis of the relationship between the number of cybercrimes and commercial banks is performed. The study offers **recommendations** to Internet users (how to recognize the signs of fraud), and to regulatory bodies on improving the system of supervision over the dissemination of information in cyberspace. The authors **concluded** that it is necessary to increase the level of cyber literacy and general literacy of the population, on the one hand, and to modernize the methods of supervision and control of the information posted on the Internet, on the other hand, to effectively counter financial and cybercrime. The research **results** can be used in the further development of remote banking services for the population to increase competitiveness in the banking services market. **Prospects** for further research on this topic lie in expanding its structure, developing the competencies of specialists in the field of remote banking technologies, as well as developing the scientific and technical potential of Russia.

Keywords: cyberspace; phishing; cybersecurity; cyber literacy; remote banking services; risks; attacker; user; fictitious organization

For citation: **Revenkov P.V., Oshmankevich K.R., Berdyugin A.A. Phishing schemes in the banking sector: Recommendations to Internet users on protection and development of regulatory tasks. *Finance: Theory and Practice.* 2021;25(6):212-226. DOI: 10.26794/2587-5671-2021-25-6-212-226**

ВВЕДЕНИЕ

В современном мире все большее количество времени люди проводят в Интернете. Благодаря развитию интернета появилась возможность не только получать необходимую информацию, но и совершать покупки, банковские переводы и платежи в режиме реального времени (online). Мировой объем информации, генерируемый людьми, государственными органами и предприятиями, возрастет к 2025 г. более чем в пять раз и составит 175 зеттабайт (чтобы получить 1 зеттабайт, нужна память 34,4 млрд дисков емкостью 32 гигабайта) по сравнению с сегодняшними 33 зеттабайтами[1].

Активное развитие информационно-коммуникационных технологий и их использование в большинстве областей человеческой деятельности делает актуальными новые вопросы обеспечения кибербезопасности и защиты информации в киберпространстве. Одновременно с этим возникает необходимость разработки новых алгоритмов и методов оценки рисков (примеры такой разработки можно найти в [1]). При этом алгоритмы и методы должны быть связаны с определенными особенностями функционирования корпоративных информационных систем коммерческих банков, включая различные варианты электронного банкинга (интернет-банкинг, мобильный банкинг и др.).

В стандарте ISO/IEC 27032:2012 киберпространство характеризуется как «комплексная среда, возникшая как результат взаимодействия пользователей, подключенных к глобальной сети Интернет, аппаратно-программного обеспечения, а также осуществляемых в этой сети услуг. Эта среда существует в виртуальной (сконструированной), а не материальной (физической) форме». При этом кибербезопасность представляет собой «сохранение конфиденциальности, целостности и доступности информации в киберпространстве»[2].

К киберпространству может быть применен закон Роберта Меткалфа, определяющий возрастание ценности (полезности) сети с ростом количества устройств, взаимосвязанных посредством сети Интернет:

$$Ц_n \approx n^2/2.$$

Объясняется это тем, что граф K_n содержит $n \cdot (n-1)/2$ ребер (коммуникаций) при n вершин (технологий). Это значение асимптотически приближается к $n^2/2$. Стоит добавить, что в экономике

[1] Эксперт: объем данных в мире к 2025 году вырастет более чем в пять раз. URL: https://tass.ru/ekonomika/6209822 (дата обращения: 10.01.2021).

[2] ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cybersecurity. International Organization for Standardization. URL: http://www.iso.org/standard/44375.html (дата обращения: 05.01.2021).

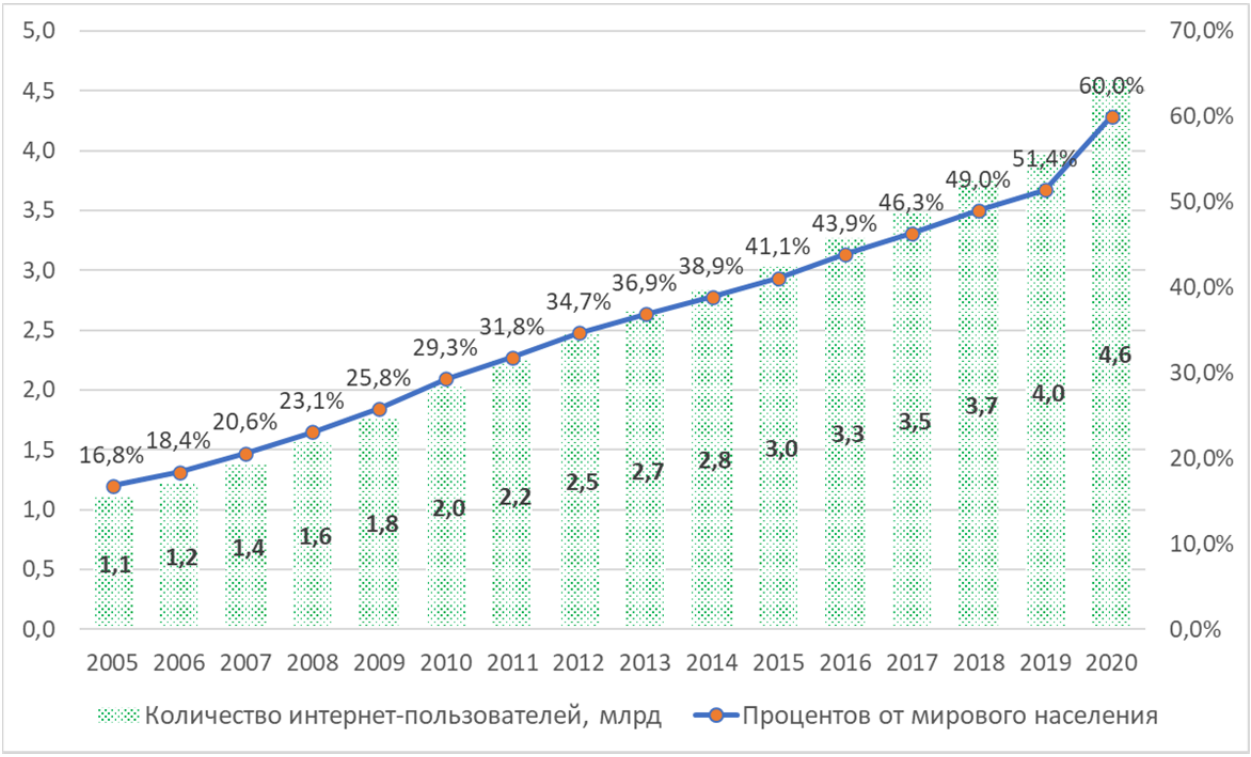

Рис. 1 / Fig. 1. **Динамика количества интернет-пользователей и их доля от мирового населения / Dynamics of the number of Internet users and their share of the world population**

Источник / Source: Интернет-доступ (мировой рынок) / Internet access (global market). URL: https://www.tadviser.ru/a/53635 (дата обращения: 10.01.2021) / (accessed on 10.01.2021).

закон Меткалфа является характеристикой положительного сетевого эффекта. К настоящему моменту интернетом пользуются более половины мирового населения (свыше 4,6 млрд человек) (*рис. 1*).

Использование хакером «отмычек» не к компьютеру, а к логике пользователя является информационно-психологическим воздействием (ИПВ, социальная инженерия). В книге [2] на многочисленных примерах охарактеризован арсенал основных средств и психологических приемов социального хакера (трансактный анализ, нейролингвистическое программирование), рассмотрены способы защиты от социального хакинга. Несмотря на некоторое моральное устаревание книги, приведенные рецепты актуальны по сей день. Особенности предоставления финансовых услуг в киберпространстве проанализированы в коллективной работе [3]. Книга посвящена методологии обеспечения кибербезопасности в технологиях электронного банкинга и минимизации рисков, возникающих при использовании дистанционного банковского обслуживания.

В монографии [4] автор (сотрудник Института США и Канады РАН) создает обширную и наполненную конкретными фактами картину рисков нарушения информационной безопасности социальной, военно-политической и экономической жизни Соединенных Штатов Америки, рост которых влечет за собой резкое увеличение воздействия объектами киберпространства на реальные формы жизни. Книга носит междисциплинарный характер: затрагивает вопросы, относящиеся к различным наукам (социологии, политологии, экономике) и убеждает читателей в правильности многопланового подхода к анализу вопросов информационного общества.

Головной мозг человека имеет нервные клетки, которые активизируются не только при выполнении определенного действия, но и при наблюдении человеком за выполнением этого действия окружающими — это зеркальные нейроны [5]. Знание о зеркальных нейронах помогло китайским исследователям в начале XXI в., когда они отправили делегацию в известные американские корпорации (Apple, Microsoft, Google), расспросив изобретателей об их образе жизни. После чего в образовательную программу Китая по литературе были включены произведения любимого жанра литературы изобретателей (научной фантастики), и сегодня разработки Alibaba, Xiaomi, Huawei находятся в числе мировых лидеров [6–7]. Воздействие на человека работ Георгия Сытина и Дейла Карнеги (библиотерапия) также обусловлено эффектом зеркальных нейронов, что впервые отмечено в этой статье.

В перечень «100 книг для школьников» от Минобрнауки России авторы статьи предлагают добавить утопический HSF-роман[3] советского ученого И.А. Ефремова «Туманность Андромеды». Как и в случае с Китаем, внимание к HSF-литературе (параллельно с развитием фундаментальных и прикладных наук) приведет к конкурентоспособному импортозамещению в сфере цифровых технологий, и Россия прославится не только военной техникой (которая преимущественно разработана в СССР [8]), но и мирной электроникой (компьютеры, смартфоны, бытовая техника). Подчеркнем, что без следования ***формальной логике*** и ***финансовой грамотности*** и научная фантастика, и фишинг остаются лишь набором софизмов.

Мотивирующей и познавательной, но не фантастической книгой, описывающей историю российских стартапов Республики Саха (Якутия), является [9]. Возникновение и развитие IT-компании Sinet Team, информационного портала Ykt.Ru и ставшего международным интернет-агрегатора услуг такси inDriver автор (основатель и генеральный директор) характеризует через призму исторических событий в России и собственного жизненного опыта. Проблемы кибербезопасности (chargeback — требование возврата платежа, который не был санкционирован настоящим владельцем карты) у якутского такси inDriver возникли лишь в Нью-Йорке.

Научно-популярная книга [10] характеризует факторы риска в различных сферах: от финансовых систем и атомных электростанций до самолетов и цифровых платформ. Авторы используют концепции сложности системы и жесткости связанности ее элементов для определения причин сбоев и нарушений систем. Развивая теорию «нормальных аварий» Чарльза Перроу (Charles Perrow), авторы анализируют произошедшие катастрофы, предлагая конкретные инструменты и практические рекомендации, которые могли бы предотвратить нежелательные последствия.

Таким образом, анализ информационной и кибербезопасности в настоящее время рассматривается довольно широко, поскольку киберпространство стало пятым театром военных действий, следующим после суши, моря, воздуха и космоса.

КИБЕРПРЕСТУПНОСТЬ В БАНКОВСКОЙ СФЕРЕ: ФИШИНГ

Наряду с появлением удобств, предоставляемых киберпространством, возникли новые способы мошенничества. Наиболее активно осуществляется мошенничество через интернет в кредитно-финансовом секторе и сфере ритейла. Это обусловлено, прежде всего, тем, что в указанных сферах злоумышленники могут получить наибольшую материальную выгоду.

Фишинг (от англ. phishing, происходит от fishing — рыбная ловля, выуживание) является одним из наиболее распространенных методов совершения мошенничества в киберпространстве, который используется для хищения паролей и конфиденциальной информации путем введения клиента в заблуждение. Обычно мошенник копирует исходный код официальной страницы (эту функцию предоставляет любой браузер) и сохраняет его в текстовом редакторе. Далее в исходном коде подменяется оригинальный URL-адрес для входа в систему на адрес программы (скрипта), где прописаны условия подмены адресов, алгоритм действий после ввода регистрационных данных и способ получения этих данных мошенником. Основные работы по созданию фишинговой страницы закончены. Имея домен и хостинг, хакер размещает свою страницу в сети Интернет и переадресует на нее пользователей [11].

В I квартале 2020 г. фишинговые рассылки были связаны с темой COVID-19. При этом на частных лиц была направлена почти половина из них (44%), а на государственные организации — каждая пятая рассылка[4].

Определим тесноту связи между статистикой Министерства внутренних дел России о преступлениях в сфере компьютерной информации, предварительное следствие по которым обязательно, и данными Центрального банка Российской Федерации о количестве кредитных организаций в России (см. *таблицу*).

Определим среднее квадратичное отклонение

$$\sigma_x \approx \sqrt{\frac{\sum_{i=1}^{n} x_i^2}{n} - \bar{x}^2} \text{ и } \sigma_y \approx \sqrt{\frac{\sum_{i=1}^{n} y_i^2}{n} - \bar{y}^2}:$$

$$\sigma_x = \sqrt{\frac{17812989}{18} - 950,2^2} \approx 294,5$$

$$\text{и } \sigma_y = \sqrt{\frac{712122038}{18} - 5354,2^2} \approx 3300,7.$$

Найдем ковариацию $C_{xy} \approx \frac{\sum_{i=1}^{n} x_i y_i}{n} - \bar{x} \cdot \bar{y}$:

[3] «Твердая» научная фантастика (от англ. hard science fiction — HSF) — поджанр научной фантастики, уделяющий внимание вопросам научно-технического прогресса.

[4] Positive Technologies: около 13% всех фишинговых атак связаны с темой COVID-19. URL: https://www.securitylab.ru/news/509238.php (дата обращения: 08.01.2021).

Таблица / Table

Данные Банка России и МВД России / Data of the Bank of Russia and the Ministry of Internal Affairs of Russia

Год / Year	Банки (X) / Banks	Преступления (Y) / Crimes	X^2	Y^2	$X \cdot Y$
2003	1329	7540	1 766 241	56 851 600	10 020 660
2004	1329	8739	1 766 241	76 370 121	11 614 131
2005	1299	10 214	1 687 401	104 325 796	13 267 986
2006	1253	8889	1 570 009	79 014 321	11 137 917
2007	1189	7236	1 413 721	52 359 696	8 603 604
2008	1136	9010	1 290 496	81 180 100	10 235 360
2009	1108	11 636	1 227 664	135 396 496	12 892 688
2010	1058	7398	1 119 364	54 730 404	7 827 084
2011	1012	2698	1 024 144	7 279 204	2 730 376
2012	978	2820	956 484	7 952 400	2 757 960
2013	956	2563	913 936	6 568 969	2 450 228
2014	923	1739	851 929	3 024 121	1 605 097
2015	834	2382	695 556	5 673 924	1 986 588
2016	733	1748	537 289	3 055 504	1 281 284
2017	623	1883	388 129	3 545 689	1 173 109
2018	490	2500	240 100	6 250 000	1 225 000
2019	442	2883	195 364	8 311 689	1 274 286
2020	411	4498	168 921	20 232 004	1 848 678
Сумма	17103	96 376	17 812 989	712 122 038	103 932 036
Средн.	950,2	5354,2	989 610,5	39 562 335,4	5 774 002

Источник / Source: Информация о банковской системе Российской Федерации. Центральный банк Российской Федерации (Банк России) / Information about the banking system of the Russian Federation. Central Bank of the Russian Federation (Bank of Russia). URL: https://www.cbr.ru/statistics/? PrtId=lic (дата обращения: 21.01.2021) / (accessed on 21.01.2021). Состояние преступности (архивные данные). Министерство внутренних дел Российской Федерации / The state of crime (archival data). Ministry of Internal Affairs of the Russian Federation. URL: https://mvd.ru/folder/101762 (дата обращения: 21.01.2021) / (accessed on 21.01.2021).

$$C_{xy} = 5\,774\,002 - 950,2 \cdot 5354,2 \approx 686\,441,16.$$

Коэффициент корреляции $r_{xy} = \dfrac{C_{xy}}{\sigma_x \sigma_y}$ равен

$$r_{xy} = \frac{686\,441,16}{294,5 \cdot 3300,7} \approx 0,71.$$

Значение корреляции $r_{xy} \approx 0,71$ подтверждает результаты прогресса и оптимизации[5]. Ликвидация финансовых «пылесосов», которые привлекают вкладчиков рискованными сделками для перевода их денег за границу, ведет к оптимизации финансовой деятельности и возрастанию надежности средств защиты банковской информации за счет развития телекоммуникационных технологий и постепенного перехода от традиционного банкинга к онлайн-платформам.

Эти явления постоянно изменяются, что усложняет процесс выявления и раскрытия совершаемых правонарушений в киберпространстве. Безусловно, в процессе развития информационных технологий появляются специальные средства и программы по выявлению и предупреждению атак на пользо-

[5] Вычисления могут быть осуществлены автоматически в программах обработки статистических данных [12], но для наглядности приведен ручной расчет.

Рис. 2 / Fig. 2. **Пример фишингового сайта фиктивного банка / Example of a phishing website of a fictitious bank**

Источник / Source: [3] и лекция генерального директора «Лаборатории Касперского» Е.В. Касперского в Финансовом университете — полная версия / [3] and lecture by Eugene V. Kaspersky, CEO of Kaspersky Lab at the Financial University — full version. URL: https://youtu.be/s2YLFXQVkPc (дата обращения 27.05.2021) / (accessed on 27.05.2021).

вателей в сети Интернет. Специалисты в области информационной безопасности делят кибератаки по следующим основным группам:

- фишинг;
- социальная инженерия (ИПВ);
- вредоносное программное обеспечение [13].

Фишинговые атаки объединяют в себе как социальную инженерию, так и использование вредоносного программного обеспечения, что делает их одним из основных и наиболее опасных способов совершения атак в сети Интернет [14].

В рамках данной статьи под фишингом мы будем понимать информационную систему, применяемую для получения от третьих лиц (пользователей системы) конфиденциальных сведений за счет введения их в заблуждение относительно ее подлинности вследствие сходства доменных имен, оформления или содержания информации[6]. На основе данного подхода к фишингу рассмотрим самые распространенные схемы мошенничества с использованием интернета.

ЛЖЕБАНКИ

Одна из самых распространенных категорий фишинговых ресурсов — это сайты фиктивных (несуществующих, фейковых) банков. Недобросовестное лицо создает ресурс «банка» и начинает привлекать денежные средства граждан и юридических лиц во вклады. Пользователь ресурса не задумывается о правомерности деятельности данного лица, поскольку интерфейс несуществующей «кредитной организации» очень похож на интерфейс действующего банка [15]. К сожалению, свобода слова иногда перерастает в свободу дезинформации.

Представленные на ресурсе поддельные документы (такие как копии лицензий и доверенностей) создают у потребителя впечатление, что данный банк является легальным (*рис. 2*).

От имени банка злоумышленники готовы предоставить различного рода кредиты. При обращении потребителя в такой банк (с просьбой предоставить ему, например, ипотечный кредит) его заявку одобряют и просят оплатить курьерскую доставку договора и страховую сумму. После внесения потребителем оплаты банк прекращает контакты с клиентом.

По официальной статистике Банка России[7], в III квартале 2020 г. было выявлено 375 сайтов лжебанков, из которых было заблокировано 95% сайтов. Стоит заметить, что количество таких несуществующих банков выросло в 3 раза по сравнению с аналогичным периодом за 2019 г. Предположительно, это связано

[6] Правила регистрации доменных имен в доменных зонах. RU и.РФ. URL: https://cctld.ru/ru/docs/project/algoritm/rules_draft.pdf (дата обращения: 17.01.2021).

[7] Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. URL: https://www.cbr.ru/analytics/ib/review_3q_2020/ (дата обращения: 01.02.2021).

с расширением потребности граждан в денежных средствах, а также расширением спектра дистанционного предоставления финансовых услуг в период пандемии COVID-19, что вызвало переориентацию мошенников в данной сфере.

Злоумышленники также активно используют наименования реально действующих банков и создают сайты-клоны или сайты-двойники, что позволяет обмануть пользователя [16].

Приведем перечень признаков фишинговых ресурсов данной категории:

1. Отсутствие информации об организации в справочниках (Реестрах) Банка России.

На официальном сайте Центрального банка Российской Федерации (URL: http://www.cbr.ru) размещены:

- Книга государственной регистрации кредитных организаций.
- Справочник по кредитным организациям.

2. Отсутствие информации об организации в соответствующих реестрах Федеральной налоговой службы Российской Федерации и Роскомнадзора.

Информацию об организации, представленную на сайте, также можно проверить в следующих реестрах:

- Единый государственный реестр юридических лиц (ЕГРЮЛ), размещенный на официальном сайте Федеральной налоговой службы (ФНС) Российской Федерации.
- Реестр операторов, осуществляющих обработку персональных данных, размещенный на официальном сайте Роскомнадзора России.

Лжебанки стали одним из самых распространенных способов мошенничества на территории России, поскольку злоумышленникам не приходится точно копировать ресурсы реально действующих кредитных организаций, достаточно оформить вкладки на сайте со следующим названием «Кредит», «Вклады» и т.д. Данные наименования позволяют ввести пользователя в заблуждение и создать у него реальное представление о том, что он находится на сайте действующего банка.

Потребителям необходимо обращать внимание на оформление ресурса: мошенники, как правило, не утруждают себя в размещении на «официальном сайте» соответствующей документации (в некоторых случаях даже не указывают номер лицензии на осуществление операций).

ЛЖЕСТРАХОВЫЕ ОРГАНИЗАЦИИ

Появление возможности оформления электронных полисов обязательного страхования автогражданской ответственности (ОСАГО) с использованием интернета не только облегчило жизнь автолюбителям, но и спровоцировало рост мошенничества в данной сфере.

В рамках рассматриваемой категории злоумышленник действует различными способами:

- создает копию ресурса реально действующей страховой компании с предложениями оформления электронных полисов ОСАГО;
- предлагает к продаже фальшивые бланки или необеспеченные бланки страховых организаций.

Потребитель либо оплачивает фальсифицированный полис ОСАГО, либо оплачивает доставку и покупает фальшивые бланки[8].

Согласно статистике ФинЦЕРТ Банка России в период с 01.09.2018 по 31.08.2019 было снято с делегирования 22 ресурса, на которых осуществлялась деятельность фиктивных страховых организаций[9].

Фишинговый сайт страховой организации позволяет создать у потребителя ложное впечатление, что покупка бланка не влечет для потребителя негативных последствий. Однако при приобретении заведомо фальшивых, пустых и недействительных бланков потребитель теряет возможность претендовать на страховое возмещение в случае наступления страхового случая.

Поддельные страховые компании становятся достаточно распространенными в России ввиду того, что потребитель старается сэкономить время и денежные средства при оформлении страхового полиса в надежде на то, что страховой случай не наступит [2].

Также на практике встречаются случаи, когда страховая компания создает ресурс и выдает себя за организацию, которая предоставляет страховые услуги. Потребитель заказывает ту или иную страховую услугу, оплачивает ее переводом на карту страховщика или на его счет. Страховщик обязуется передать страховой полис или предоставить иную услугу в определенное время, но так и не передает предложенные полис или услугу потребителю (*рис. 3*).

В связи с этим потребитель должен не только обращать внимание на оформление и содержание ресурса страховой компании, но и проверять данную организацию в соответствующих справочниках

[8] После чего по ст. 327 «Подделка, изготовление или оборот поддельных документов, государственных наград, штампов, печатей или бланков» Уголовного кодекса Российской Федерации придется отвечать как продавцам, так и покупателям.

[9] См. подробнее «Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России», размещенный на официальном сайте Банка России. URL: https://cbr.ru/Content/Document/File/84354/FINCERT_report_20191010.PDF (дата обращения: 02.02.2021).

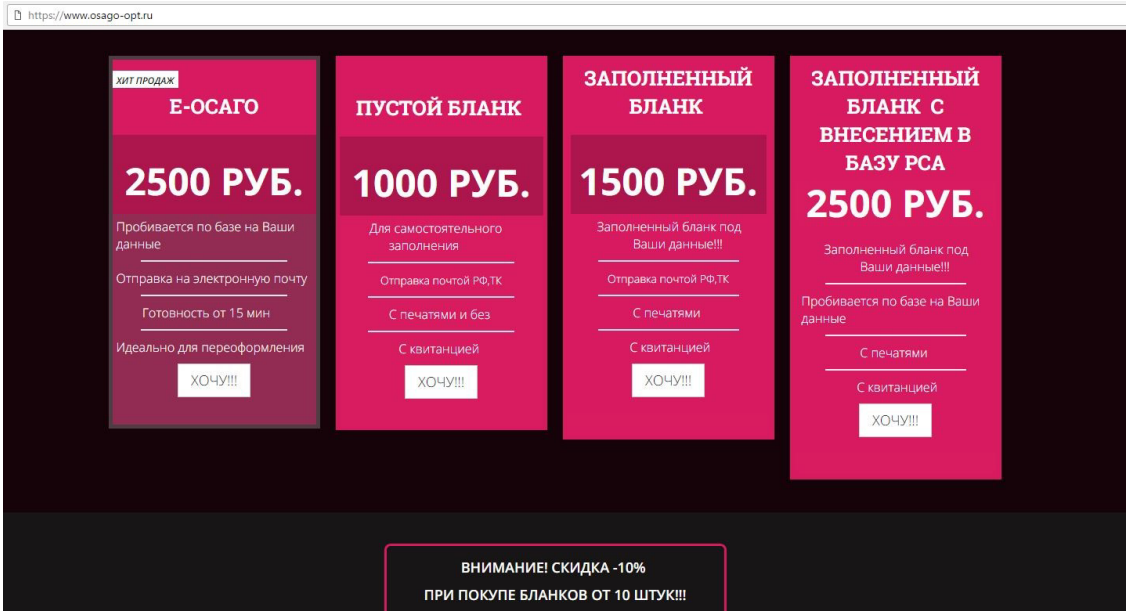

Рис. 3 / Fig. 3. **Пример фишингового сайта фиктивной страховой компании / Example of a phishing website of a fictitious insurance company**

Источник / Source: [3] и лекция генерального директора «Лаборатории Касперского» Е.В. Касперского в Финансовом университете — полная версия / [3] and lecture by Eugene V. Kaspersky, CEO of Kaspersky Lab at the Financial University — full version. URL: https://youtu.be/s2YLFXQVkPc (дата обращения: 28.05.2021) / (accessed on 28.05.2021).

и реестрах (в Справочнике участников финансового рынка Банка России[10], в перечне Российского союза автостраховщиков[11]).

ПСЕВДО-P2P (PEER-TO-PEER)

Данная категория является одной из самых привлекательных для злоумышленников, что обусловлено простотой оформления информационного ресурса для хищения денежных средств. Злоумышленники, используя этот способ, получают конфиденциальные сведения как платежной карточки, так и самого потребителя. Согласно статистике ФинЦЕРТ Банка России, в период с 01.09.2018 по 31.08.2019 г. было снято с делегирования 132 сайта, которые выдавали себя за ресурсы, предоставляющие услуги по переводу денежных средств с карты на карту[12].

Простота оформления информационных ресурсов, предоставляющих услуги по P2P-переводам, позволяет мошенникам достаточно легко их подделывать: оформляется изображение пластиковых карт, а также указываются эмблемы и наименования платежных систем или кредитной организации. Данные атрибуты позволяют сформировать у потребителя ложное представление о том, что он находится на сайте реально действующей организации (*рис. 4*).

Отметим тот факт, что пользователь передает злоумышленникам не только свои персональные данные, но и номер платежной карты третьего лица, которому он осуществляет дистанционный перевод.

Подобные ресурсы являются очень заманчивыми для потребителей, поскольку предлагают услуги по беспроцентному переводу или переводу с низким процентом денежных средств между платежными картами разных банков или платежных систем [17].

Избегать использования недобросовестных ресурсов поможет проверка наличия организации в Реестре операторов платежных систем Банка России, а также использование при осуществлении перевода защищенного соединения.

При этом, если на ресурсе указано, что услуги предоставляются какой-либо кредитной организацией, то необходимо проверить наличие данной организации в соответствующем перечне Банка России.

[10] Справочник участников финансового рынка Банка России. URL: http://www.cbr.ru (дата обращения: 02.02.2021).

[11] Присутствует ли Web-адрес организации в перечне Российского союза автостраховщиков. URL: https://www.autoins.ru/e-osago/chleny-rsa-osushchestvlyayushchie-oformlenie-elektronnykh-polisov/ (дата обращения: 02.02.2021).

[12] См. подробнее «Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России». Официальный сайт Банка России. URL: https://cbr.ru/Content/Document/File/84354/FINCERT_report_20191010.PDF (дата обращения: 02.02.2021).

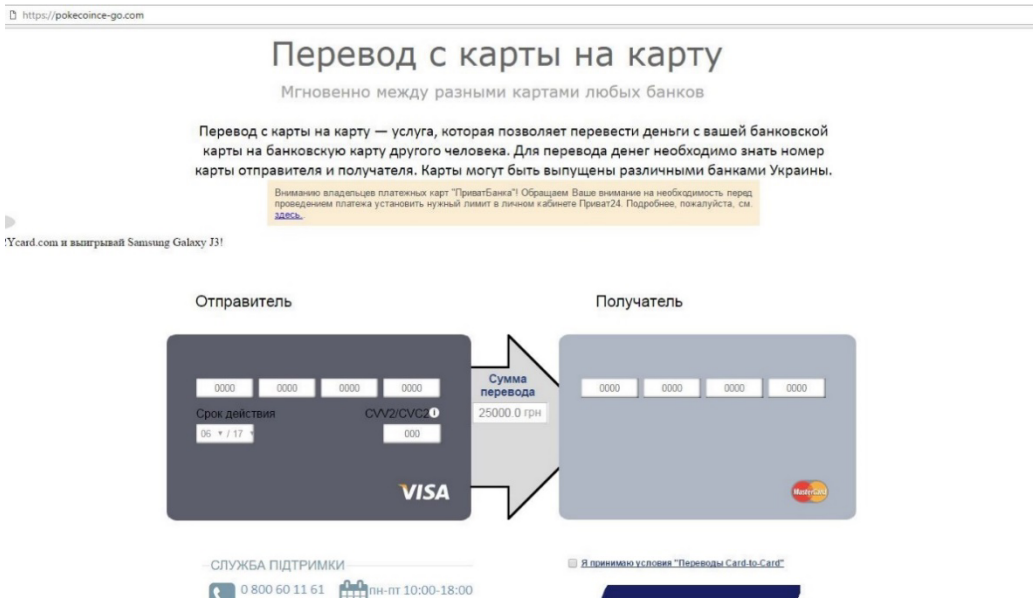

Рис. 4 / Fig. 4. **Пример фишингового сайта фиктивной системы P2P / Example of a phishing website of a fictitious P2P system**

Источник / Source: [3] и лекция генерального директора «Лаборатории Касперского» Е.В. Касперского в Финансовом университете — полная версия / [3] and lecture by Eugene V. Kaspersky, CEO of Kaspersky Lab at the Financial University — full version. URL: https://youtu.be/s2YLFXQVkPc (дата обращения 29.05.2021) / (accessed on 29.05.2021).

ЛЖЕМАГАЗИНЫ

Интернет-магазины привлекают покупателей своими ценами (за счет экономии на аренде помещений), а также возможностью удобной доставки[13]. Схема мошенничества в данном случае прежняя: как только покупатель переводит свои деньги на счет продавца, связь с ним прекращается (Web-сайт магазина перестает работать, ответа по электронной почте нет).

Оформление и содержание ресурсов также аналогичны сайтам действующих организаций (*рис. 5*) [18].

Для того чтобы обезопасить себя и приобрести соответствующий товар, потребителю необходимо проверить информацию об организации, которая предоставляет товары или услуги, указанную на сайте[14], а также отзывы и доменное имя в поисковой системе.

МОШЕННИЧЕСТВО

Данная категория является обобщающей. В ней собраны схемы мошенничества, которые осуществляются организациями с использованием сети Интернет. Эти схемы мошеннической деятельности фиктивных организаций можно разделить на следующие подвиды:

- организация, проводящая псевдоопросы под предлогом выплаты денежных средств;
- организация, осуществляющая устройство на работу;
- организация, предлагающая оформить выплату несуществующей компенсации (*рис. 6*) [19];
- организация, оформляющая «Сертификат о вакцинации против новой коронавирусной инфекции (COVID-19)»[15].

Злоумышленники привлекают пользователей за счет предоставления возможности получения быстрого заработка. Пользователи, рассчитывая на это, передают персональные данные злоумышленникам, в том числе данные банковских карт, для перечисления обещаемой им заработной платы[16].

Интерфейс ресурсов данной категории является идентичным интерфейсам официальных ресурсов,

[13] В ряде случаев продавец обосновывает эти цены, иногда совсем не скрывая таких фактов, как «товар краденый», «конфискованный» и т.п. Поэтому если жертва и решит покупать такой товар, то вряд ли потом пойдет жаловаться, так как, по сути, является соучастником преступления (скупка краденого).

[14] Данную информацию можно проверить на официальном сайте ЕГРЮЛ ФНС Российской Федерации. URL: https://egrul.nalog.ru (дата обращения: 26.10.2021).

[15] «Один в один с оригиналом»: как мошенники продают в России ковид-паспорта. URL: https://ria.ru/20210303/covid-1599609177.html (дата обращения: 14.03.2021).

[16] Нередки случаи, когда для устройства на несуществующую работу гражданам предлагается оплатить страховой взнос для предоставления заказов или же для фиксирования выплат либо предлагается осуществить оплату доставки трудового договора.

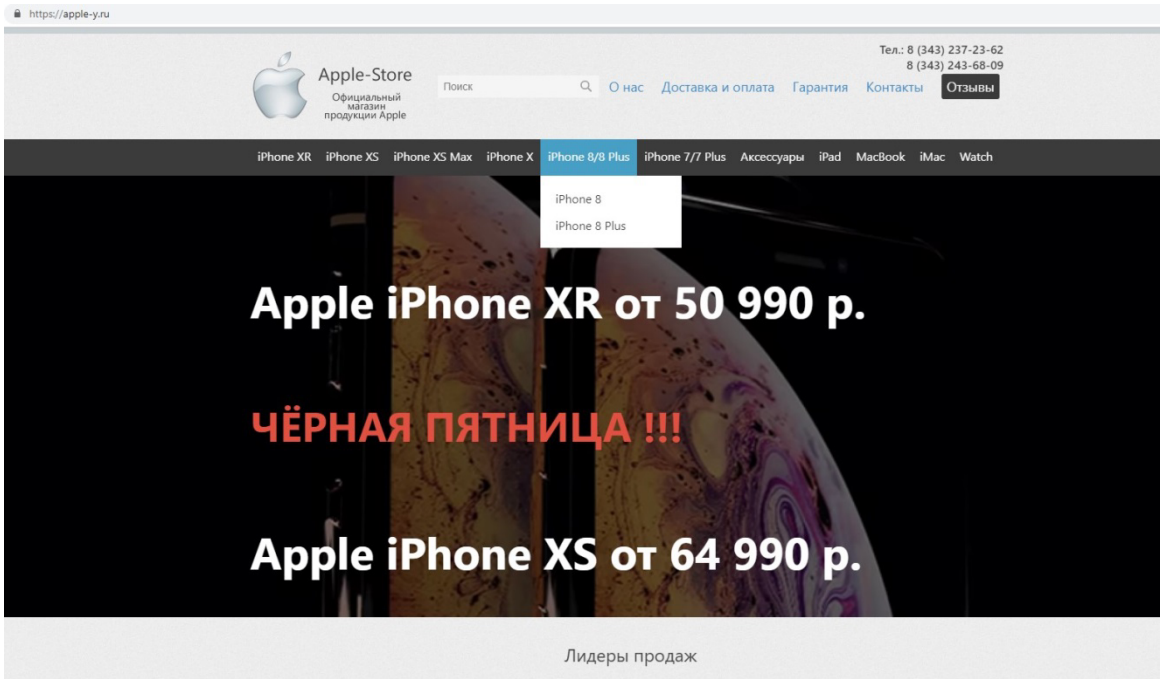

Рис. 5 / Fig. 5. **Пример фишингового сайта фиктивного интернет-магазина / Example of a phishing website of a fictitious online store**

Источник / Source: [3] и лекция генерального директора «Лаборатории Касперского» Е.В. Касперского в Финансовом университете — полная версия / [3] and lecture by Eugene V. Kaspersky, CEO of Kaspersky Lab at the Financial University — full version. URL: https://youtu.be/s2YLFXQVkPc (дата обращения: 01.06.2021) / (accessed on 01.06.2021).

что позволяет ввести клиента в заблуждение относительно получения дохода.

Пользователь на данном ресурсе проходит опрос (тест), который состоит из 7–10 простых вопросов. После прохождения опроса ресурс генерирует фейковый выигрыш и предлагает пользователю перевести денежные средства на его платежную карту. С целью сохранения денежных средств и оформления их вывода на ресурсе предлагается заплатить закрепительный платеж[17]. Пользователь предоставляет данные карт злоумышленникам и персональные данные, что позволяет аферистам списать денежные средства с его платежной карты [20].

Кроме опросов мошенники предлагают получить различные компенсации (например, за медицинские услуги). Как правило, на ресурсе размещается несуществующая документация Правительства Российской Федерации, позволяющая осуществить возврат и выплатить компенсацию населению.

Активно на данную категорию ресурсов завлекают пользователей (зачастую пенсионеров) за счет звонков и SMS-рассылок, в которых граждан убеждают в том, что компенсация предоставляется в рамках одной из федеральных программ и что она не поддается огласке общественности, поскольку существует лимит по выплатам.

Необходимо обратить внимание на то, что опросы и компенсации могут проводиться и реально действующими организациями, и государственными службами. Для того чтобы не стать жертвой мошенников, необходимо обратить внимание на следующие признаки, которые чаще всего указывают на мошеннический характер деятельности ресурса данной категории:

- перечисление денежных средств третьим лицам в счет оплаты;
- отсутствие организации в ЕГРЮЛ ФНС России;
- осуществление деятельности, не предусмотренной лицензией (разрешением);
- отзывы реальных людей об организации, найденные в поисковых системах (Яндекс, Google).

Противодействие данному виду мошенничества осуществляется не только правоохранительными, но и регулирующими органами. В соответствии с нормативно-правовыми актами Банка России кредитные и некредитные финансовые организации информируют Банк России при выявлении инцидентов информационной и финансовой без-

[17] Сумма платежа является незначительной и составляет от 250 до 1000 рублей.

Рис. 6 / Fig. 6. **Пример фишингового сайта с информацией «о выплатах компенсации» / Example of a phishing website with information about payments of non-existent compensation**

Источник / Source: [3] и лекция генерального директора «Лаборатории Касперского» Е.В. Касперского в Финансовом университете — полная версия / [3] and lecture by Eugene V. Kaspersky, CEO of Kaspersky Lab at the Financial University — full version. URL: https://youtu.be/s2YLFXQVkPc (дата обращения: 02.06.2021) / (accessed on 02.06.2021).

опасности[18], а также уведомляют о выявленных фишинговых ресурсах [21].

Надзорные мероприятия со стороны Банка России и Роскомнадзора направлены, прежде всего, на обеспечение стабильности финансовой системы и защиты кредиторов и вкладчиков. В основе такой деятельности лежит комплексный подход: соблюдение нормативных актов, своевременное уведомление Банка России и комплексный анализ в рамках надзорных мероприятий позволяют кредитным и некредитным финансовым организациям минимизировать риски наступления неблагоприятных последствий как для них самих, так и для их клиентов, а также повысить уровень информационной безопасности и защищенности.

СОВЕРШЕНСТВОВАНИЕ КОНТРОЛЯ В КИБЕРПРОСТРАНСТВЕ

Учитывая активное использование киберпространства при предоставлении различного рода банковских слуг, необходимо понимать, что перед регулирующими органами встает достаточно сложная задача — построить эффективный надзор за достоверностью информации, размещаемой на Web-представительствах организаций кредитно-финансовой сферы. Очевидно, что такая работа должна проводиться при активном взаимодействии с правоохранительными органами, чтобы своевременно принимать меры по недопущению мошеннических действий (в кратчайшие сроки закрывать мошеннические ресурсы и принимать меры к привлечению к ответственности виновных лиц) [3, 22].

Немаловажная роль в снижении киберпреступности отводится и повышению общего уровня киберграмотности всех слоев населения (*рис. 7*). Одним из наиболее эффективных способов является включение в образовательные программы для учащихся средних и высших учебных заведений специализированных дисциплин (курсов), на которых учащиеся будут получать знания в области функционирования новых финансовых технологий, а также об основных способах обеспечения кибербезопасности (включая отдельные темы по противодействию кибермошенничеству).

Дополнительно знакомство с литературой, рассмотренной в первой части статьи «Введение и анализ литературы», будет способствовать повышению

[18] См. подробнее положение Банка России от 09.06.2012 № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств», положение Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента», положение Банка России от 17.04.2019 № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».

Рис. 7 / Fig. 7. **Мероприятия по контролю в киберпространстве / Measures to control cyberspace**
Источник / Source: составлено авторами / complied by the authors.

уровня киберграмотности и общей грамотности населения. С начала июня 2021 г. Банк России публикует список компаний с выявленными признаками нелегальной деятельности на финансовом рынке (так называемый «черный» список): https://cbr.ru/inside/warning-list/, куда относятся, в том числе, и фишинговые компании. Если организация числится в этом списке, то лучше игнорировать ее услуги и уходить. Если клиент столкнулся с мошеннической компанией и ее нет в списке, то он может сообщить о ней[19].

Профилактика фишинга заключается также в ознакомлении с телепередачами типа «Расследование Эдуарда Петрова. Интернет-пандемия, или Секта "COVID-19" — Россия 24» (URL: https://youtu.be/0hklRanOSxI) и «Финал Finiko. Специальный репортаж — Россия 24» (URL: https://youtu.be/5OtEZtLw9bE), где иллюстрируются результаты человеческой веры в волшебные пилюли и финансовые пирамиды[20]. Таким образом, будет развита система контроля в виртуальном пространстве, а также поднята культура поведения всех участников киберпространства.

ВЫВОДЫ

Вклад в развитие теоретической и прикладной науки заключается в адаптации решений для развития научно-технического прогресса России на основе позитивного опыта Китая, а также в расширении методологического аппарата информационной безопасности и киберграмотности.

Новая реальность и вызовы кибербезопасности, с которыми вынуждены сталкиваться как организации кредитно-финансовой сферы, так и их клиенты при использовании технологий дистанционного банковского обслуживания, требуют модернизации, а в ряде случаев — и значительного пересмотра процедур управления рисками, включая новые процедуры контроля информации, размещаемой на Web-представительствах (сайтах) организаций [15]. Также

[19] Подробнее: «ЦБ опубликовал черный список из 1,8 тыс. нелегальных компаний». URL: https://www.rbc.ru/finances/01/06/2021/60b5fbdc9a79471a267396e1 (дата обращения: 25.07.2021).

[20] Превзойти существующие сегодня методы фишинга могут только набирающие популярность фейки о чудотворном эффекте употребления… мухоморов (см. URL: https://smotrim.ru/article/2639202).

необходимо повышение уровня киберграмотности различных слоев населения.

Отставание в вопросах киберграмотности становится основной причиной хищений денежных средств у клиентов организаций кредитно-финансовой сферы. В связи с этим необходимо использовать различные каналы связи и средства массовой информации для оповещения клиентов о потенциальных угрозах со стороны кибермошенников, наиболее характерных видах кибератак и методах социальной инженерии[21]. Такая работа позволит значительно снизить уровень кибермошенничества и свести его к минимуму. Регулирующим органам следует совершенствовать способы осуществления надзора и контроля за размещаемой информацией в сети Интернет. Результатом такой деятельности станет не только повышение доверия со стороны клиентов и пользователей интернета к технологиям дистанционного банковского обслуживания, но и повышение доверия к кредитно-финансовой сфере в целом.

[21] По данной тематике Банк России выпустил рекомендации для кредитных организаций от 19.02.2021 № 3-МР «Методические рекомендации по усилению кредитными организациями информационной работы с клиентами в целях противодействия несанкционированным операциям». URL: /statichtml/file/117596/20210219_3-mr.pdf (дата обращения: 02.02.2021).

СПИСОК ИСТОЧНИКОВ

1. Бердюгин А.А., Ревенков П.В. Оценка риска воздействия кибератак в технологиях электронного банкинга (пример программной реализации). *Финансы: теория и практика = Finance: Theory and Practice*. 2020;24(6):51–60. DOI: 10.26794/25875671–2020–24–6–51–60
2. Кузнецов М.В., Симдянов И.В. Социальная инженерия и социальные хакеры. СПб.: БХВ-Петербург; 2007. 368 с. URL: https://www.koob.ru/kuznetsov_m/social_engineering (дата обращения: 27.07.2021).
3. Конявская С.В., Ревенков П.В., Русин Л.И. и др. Кибербезопасность в условиях электронного банкинга: практическое пособие. М.: Прометей; 2020. 522 с.
4. Роговский Е.А. Кибер-Вашингтон: глобальные амбиции. М.: Международные отношения; 2014. 848 с.
5. Bushov Y., Ushakov V., Svetlik M., Esipenko E., Kartashov S., Orlov V., Malakhov D. Activity of mirror neurons in man in the observation, pronunciation and mental pronunciation of words. *Procedia Computer Science*, 2020;169:100–109. DOI: 10.1016/j.procs.2020.02.121
6. Долинго Б.А. Фантастика — самый мощный инструмент развития воображения. *Наука и жизнь*. 2016;6:118–121. URL: https://www.nkj.ru/archive/articles/28924/ (дата обращения 27.01.2021).
7. Ошманкевич К.Р. Особенности правового регулирования банковской системы и банковского надзора в китайской народной республике. *Вестник Московского университета. Серия 26: Государственный аудит*, 2020;1:50–59.
8. Сорокин Д.Е. Политическая экономия технологической модернизации России. *Экономическое возрождение России = Economic revival of Russia*. 2020;1(63):18–25. URL: https://www.elibrary.ru/item.asp?id=42543826 (дата обращения: 05.08.2021).
9. Томский А.Г. inDriver: От Якутска до Кремниевой долины. История создания глобальной технологической компании. М.: Альпина Паблишер; 2020. 256 с.
10. Clearfield C., Tilcsik A. Meltdown: Why Our Systems Fail and What We Can Do About It. Penguin Press; 2018. 304 p.
11. Vincent A. Don't feed the phish: how to avoid phishing attacks. *Network Security*. 2019;2:11–14. DOI: 10.1016/S 1353–4858(19)30022–4
12. Каганов В.И. Компьютерные вычисления в средах Excel и Mathcad. М.: Горячая линия — Телеком; 2015. 328 с.
13. Добрышин М.М., Закалкин П.В. Модель компьютерной атаки типа "Phishing" на локальную компьютерную сеть. *Вопросы кибербезопасности*. 2021;2(42):17–25. DOI: 10.21681/2311–3456–2021–2–17–25
14. Salihu A., Metin H., Hajrizi E., Ahmeti M. The Effect of Security and Ease of Use on reducing the problems/deficiencies of Electronic Banking Services. *IFAC-PapersOnLine*. 2019;52(25):159–163. DOI: 10.1016/j.ifacol.2019.12.465
15. Эскиндаров М.А., Соловьев В.И., ред. Парадигмы цифровой экономики: Технологии искусственного интеллекта в финансах и финтехе. М.: Когито-Центр; 2019. 325 с.
16. Grassegger T., Nedbal D. The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering. *Procedia Computer Science*. 2021;181:59–66. DOI: 10.1016/j.procs.2021.01.103
17. Derek S. Reveron, John E. Savage. Cybersecurity Convergence: Digital Human and National Security. *Orbis*. 2020;64(4):555–570. DOI: 10.1016/j.orbis.2020.08.005

18. Mitnick K., Vamosi R. The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data. Little, Brown and Company; 2017. 320 p.
19. Hadnagy C. Social Engineering: The Science of Human Hacking. Wiley publ.; 2018. 320 p.
20. Buldas A., Gadyatskaya O., Lenin A., Mauw S., Trujillo-Rasua R. Attribute evaluation on attack trees with incomplete information: a preprint. *Computers & Security*. 2020;88:1–21. URL: https://arxiv.org/abs/1812.10754 (accessed on 28.02.2021).
21. Фрумина С.В. Развитие цифровой экономики: опыт России и Германии. *Финансы и кредит*. 2019;25(2):263–276. DOI: 10.24891/fc.25.2.263
22. Salloum S., Gaber T., Vadera S., Shaalan K. Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey. *Procedia Computer Science*. 2021;189:19–28. DOI: 10.1016/j.procs.2021.05.077

REFERENCES

1. Berdyugin A.A., Revenkov P.V. Cyberattack Risk Assessment in Electronic banking Technologies (the Case of Software Implementation). *Finance: Theory and Practice*. 2020;24(6):51–60. (In Russ.). DOI: 10.26794/25875671–2020–24–6–51–60
2. Kuznetsov M.V., Simdyanov I.V. Social engineering and social hackers. St. Petersburg: BHV-Petersburg; 2007. 368 p. URL: https://www.koob.ru/kuznetsov_m/social_engineering (accessed on 27.07.2021). (In Russ.).
3. Konyavskaya S.V., Revenkov P.V., Rusin L.I. et al. Cybersecurity in the conditions of electronic banking: Practical guide. Moscow: Prometei; 2020. 522 p. (In Russ.).
4. Rogovsky E.A. Cyber-Washington: global ambitions. Moscow: International relations; 2014. 848 p. (In Russ.).
5. Bushov Y., Ushakov V., Svetlik M., Esipenko E., Kartashov S., Orlov V., Malakhov D. Activity of mirror neurons in man in the observation, pronunciation and mental pronunciation of words. *Procedia Computer Science*, 2020;169:100–109. DOI: 10.1016/j.procs.2020.02.121
6. Dolingo B.A. Science fiction is the most powerful tool for the development of imagination. *Nauka i zhizn' = Science and Life*. 2016;6:118–121. URL: https://www.nkj.ru/archive/articles/28924/ (accessed on 27.01.2021). (In Russ.).
7. Osmankevich K.R. Features of legal regulation of the banking system and banking supervision in the People's Republic of China. *Bulletin of the Moscow University. Series 26: State Audit*, 2020;1:50–59.
8. Sorokin D.E. Political economy of Russia's technological modernization. *Ekonomicheskoye vozrozhdeniye Rossii = Economic revival of Russia*. 2020;1(63):18–25. URL: https://www.elibrary.ru/item.asp?id=42543826 (accessed on 05.08.2021). (In Russ.).
9. Tomsky A.G. inDriver: From Yakutsk to Silicon Valley. The history of the creation of a global technology company. Moscow: Alpina Publisher; 2020. 256 p. (In Russ.).
10. Clearfield C., Tilcsik A. Meltdown: Why Our Systems Fail and What We Can Do About It. Penguin Press; 2018. 304 p.
11. Vincent A. Don't feed the phish: how to avoid phishing attacks. *Network Security*. 2019;2:11–14. DOI: 10.1016/S 1353–4858(19)30022–4
12. Kaganov V.I. Computer calculations in Excel and Mathcad environments. Moscow: Hotline — Telecom; 2015. 328 p. (In Russ.).
13. Dobryshin M.M, Zakalkin P.V. Model of a "Phishing" type of computer attack on a local computer network. *Cybersecurity issues = Voprosy kiberbezopasnosti*. 2021;2(42):17–25. (In Russ.). DOI: 10.21681/2311–3456–2021–2–17–25
14. Salihu A., Metin H., Hajrizi E., Ahmeti M. The Effect of Security and Ease of Use on reducing the problems/deficiencies of Electronic Banking Services. *IFAC-PapersOnLine*. 2019;52(25):159–163. DOI: 10.1016/j.ifacol.2019.12.465
15. Eskindarov M.A., Solov'ev V.I., eds. Paradigms of the digital economy: Artificial intelligence technologies in finance and fintech. Moscow: Cogito-Center; 2019. 325 p. (In Russ.).
16. Grassegger T., Nedbal D. The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering. *Procedia Computer Science*. 2021;181:59–66. DOI: 10.1016/j.procs.2021.01.103
17. Derek S. Reveron, John E. Savage. Cybersecurity Convergence: Digital Human and National Security. *Orbis*. 2020;64(4):555–570. DOI: 10.1016/j.orbis.2020.08.005
18. Mitnick K., Vamosi R. The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data. Little, Brown and Company; 2017. 320 p.
19. Hadnagy C. Social Engineering: The Science of Human Hacking. Wiley publ.; 2018. 320 p.

20. Buldas A., Gadyatskaya O., Lenin A., Mauw S., Trujillo-Rasua R. Attribute evaluation on attack trees with incomplete information: a preprint. *Computers & Security*. 2020;88:1–21. URL: https://arxiv.org/abs/1812.10754 (accessed on 28.02.2021).
21. Frumina S.V. Developing the digital economy: Experience of Russia and Germany. *Finansy i kredit = Finance and credit*. 2019;25(2):263–276. (In Russ.). DOI: 10.24891/fc.25.2.263
22. Salloum S., Gaber T., Vadera S., Shaalan K. Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey. *Procedia Computer Science*. 2021;189:19–28. DOI: 10.1016/j.procs.2021.05.077

ИНФОРМАЦИЯ ОБ АВТОРАХ / ABOUT THE AUTHORS

Павел Владимирович Ревенков — доктор экономических наук, профессор Департамента информационной безопасности, Финансовый университет, Москва, Россия
Pavel V. Revenkov — Dr. Sci. (Econ.), Prof., Department of Information Security, Financial University, Moscow, Russia
pavel.revenkov@mail.ru

Ксения Романовна Ошманкевич — преподаватель института информационных наук, Московский государственный лингвистический университет, Москва, Россия
Kseniya R. Oshmankevich — lecturer of the Information Sciences Institute,
Moscow State Linguistic University, Moscow, Russia
osh-ksenia94@mail.ru

Александр Александрович Бердюгин — младший научный сотрудник департамента информационной безопасности, Финансовый университет, Москва, Россия
Aleksandr A. Berdyugin — junior researcher, Department of Information Security, Moscow, Russia
AABerdyugin@fa.ru

Заявленный вклад авторов:
Ревенков П.В. — постановка задачи исследования, разработка концепции статьи, проверка результатов и выводов.
Ошманкевич К.Р. — результаты исследования, графическое представление материала, формирование рекомендаций и выводов.
Бердюгин А.А. — введение и анализ литературы, табличные данные и корреляционный анализ, корректура текста.

Authors' declared contribution:
Revenkov P.V. — the setting of the research task, development of the concept of the article, verification of the results and conclusions.
Oshmankevich K.R. — the results of the research, graphical representation of the material, formation of recommendations and conclusions.
Berdyugin A.A. — introduction and analysis of the literature, tabular data and correlation analysis, text proofreading.

Статья поступила в редакцию 24.02.2021; после рецензирования 09.03.2021; принята к публикации 22.09.2021.
Авторы прочитали и одобрили окончательный вариант рукописи.
The article was submitted on 24.02.2021; revised on 09.03.2021 and accepted for publication on 22.09.2021.
The authors read and approved the final version of the manuscript.