Александр А. Бердюгин
Финансовый университет при Правительстве Российской Федерации
(Финансовый университет),
Щербаковская ул., 38, Москва, 105187, Россия
e-mail: brdgn@bk.ru, <https://orcid.org/0000-0003-2301-1776>

РЕИНЖИНИРИНГ БИЗНЕС-ПРОЦЕССОВ КОММЕРЧЕСКОГО БАНКА
В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ
DOI: <http://dx.doi.org/10.26583/bit.2021.1.05>

Аннотация. Актуальность темы статьи обусловлена отсутствием научно-практической проработки вопросов реорганизации труда в кредитно-финансовом учреждении с учетом развития технологий и киберпреступности. Объект исследования – деятельность кредитной организации. Предмет – реинжиниринг бизнес-процессов банка, являющийся альтернативой методикам «Шесть сигм» и «Кайдзен». Цель этих методик – повышение качества бизнес-процессов коммерческого банка и минимизация количества ошибок операционной деятельности. Проведенный обзор источников позволил определить требования к обеспечению кибербезопасности и повышению доверия клиентов к технологиям электронного банкинга. Проанализирована динамика развития стран мира по их готовности перехода к электронному правительству в зависимости от значения валового национального продукта на душу населения. В качестве ключевого показателя деятельности предприятия разработан метод оценки для вычисления размера штрафа киберпреступникам. Приведен пример количественной оценки штрафа. Анализируемый реинжиниринг бизнес-процесса коммерческого банка направлен на улучшение процесса работы клиента и сотрудника банка за компьютером. Исследована и обоснована необходимость внедрения метода скоростного набора текста (смежная с кибербезопасностью тема) в образовательную программу России. Результаты исследования могут использоваться для дальнейших практических разработок риск-менеджмента кредитных организаций, использующих технологии электронного банкинга.

Ключевые слова: реинжиниринг бизнес-процессов, технологии электронного банкинга, риск воздействия кибератак, информационная безопасность, метод скоростной печати.

Для цитирования: БЕРДЮГИН, Александр А. РЕИНЖИНИРИНГ БИЗНЕС-ПРОЦЕССОВ КОММЕРЧЕСКОГО БАНКА В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ. Безопасность информационных технологий, [S.l.], v. 28, n. 1, p. 62–73, jan. 2021. ISSN 2074-7136. Доступно на: <<https://bit.mephi.ru/index.php/bit/article/view/1319>>. Дата доступа: 03 feb. 2021. DOI: <http://dx.doi.org/10.26583/bit.2021.1.05>.

Alexander A. Berdyugin
Financial University under the Government of the Russian Federation (Financial University),
Scherbakovskaya str., 38, Moscow, 105187, Russia
e-mail: brdgn@bk.ru, <https://orcid.org/0000-0003-2301-1776>

Reengineering of business processes of a commercial bank in the information space
DOI: <http://dx.doi.org/10.26583/bit.2021.1.05>

Abstract. The need in this research arises since issues of labor reorganization in a financial institution has not been elaborated and studied scientifically and practically, considering development of technology and cybercrime. The article deals with reorganization of labor in a credit and financial institution. The object of research is the operations of a credit institution. The subject is reengineering of business processes of a Bank, which is an alternative to the “Six Sigma” and “Kaizen” methods. The purpose of these methods is to improve the quality of business processes of a commercial bank minimizing the number of operational errors. The review of sources made it possible to determine the requirements for ensuring cybersecurity and increasing customer confidence in electronic banking technologies. Development dynamics of the countries of the world according to their readiness of transition to e-government, depending on the value of the gross national product per capita, is analyzed. As a key performance indicator of the company, an

assessment method has been developed for calculate the amount of fine for cybercriminals. An example of a quantitative assessment of the penalty is given. The studied reengineering of the business process of a commercial bank is aimed at improving the process of work of the client and the bank employee at the computer. The necessity of introducing the method of high-speed typing (a topic related to cybersecurity) in the educational program of Russia is investigated and justified. The research results may be of further use for the development of risk management in credit institutions using electronic banking technologies.

Keywords: reengineering of business processes, electronic banking technologies, the risk of cyberattacks, information security, high-speed printing method.

For citation: BERDYUGIN, Alexander A. Reengineering of business processes of a commercial bank in the information space. IT Security (Russia), [S.l.], v. 28, n. 1, p. 62–73, jan. 2021. ISSN 2074-7136. Available at: <<https://bit.mephi.ru/index.php/bit/article/view/1319>>. Date accessed: 03 feb. 2021. DOI: <http://dx.doi.org/10.26583/bit.2021.1.05>.

Введение

Цифровая революция является эпохой в истории человечества, где все связаны друг с другом онлайн, все имеют доступ к цифровым финансовым услугам. Значительная часть IT-бюджета банка расходуется на техническое обслуживание, а не на инновации [1]. По прогнозам Международной корпорации данных (IDC), к 2020 г. на услуги, оборудование и программное обеспечение кибербезопасности будет затрачено до 101,6 млрд долл. Это на 38% больше, чем 73,7 млрд долл. в 2016 г. [2]. По другим данным, уже в 2019 г. мировой рынок информационной безопасности достиг 119,9 млрд долл¹.

В работе [3] считают, что сдерживает использование технологий электронного банкинга (ТЭБ) три аспекта:

1. Сомнения клиентов в возможностях и защищенности финансовых технологий по причине компьютерной преступности и низкой надежности аппаратно-программного обеспечения ТЭБ;

2. Низкие показатели качества обеспечения дистанционных банковских услуг и удобства программного продукта;

3. Недостаточный уровень финансовой и компьютерной грамотности клиента ТЭБ.

Необходимость улучшений по этим направлениям не утратила актуальности и в настоящее время. Однако, по мнению автора, нужна реконструкция бизнес-модели, чему посвящен реинжиниринг бизнес-процессов в сфере информационных технологий коммерческого банка.

1. Обзор материалов по теме исследования

В работе используется определение «Риск воздействия кибератак» (РВКа) при наличии общепризнанных «риск нарушения информационной безопасности» или «риск кибербезопасности». Данный термин введен в [4–5].

Существующие возможности позволяют выбирать те решения по обеспечению информационной безопасности ТЭБ, которые смогут обеспечить наиболее комфортную деятельность в цифровом операционном пространстве банка и эффективное осуществление корпоративного контроля и менеджмента. Кредитные организации России должны выбирать комплементарные (взаимодополняющие) решения, которые охватывают корпоративный менеджмент в цифровой сфере и цифровую среду кредитно-финансовой организации (рис. 1).

Целями деятельности комиссии COSO (англ. The Committee of Sponsoring Organizations of the Treadway Commission, USA) является изучение факторов, которые

---

¹Информационная безопасность (мировой рынок). Портал по теме корпоративной информатизации. URL: <https://www.tadviser.ru/a/275984> (дата обращения: 10.12.2020).

способны приводить к мошенничеству с финансовой отчетностью, а также выработка рекомендаций по обеспечению информационной безопасности организации и действий по важнейшим аспектам управления организацией, внутреннего контроля, минимизации рисков компаний и противодействия мошенничеству.

COSO – The Committee of Sponsoring Organizations of the Treadway Commission (Комитет спонсорских организаций);

CPSS (КПРС) – Committee on Payment and Settlement Systems, Комитет по платежным и расчетным системам Банка международных расчетов (Bank for International Settlements – BIS);

СТО БР ИББС – стандарты Банка России по обеспечению информационной безопасности банков страны;

ISO 9000 – стандарты Международной организации стандартизации по менеджменту качества;

ISO 270xx – стандарты Международной организации стандартизации по управлению информационной безопасностью;

PCI DSS – стандарт безопасности данных индустрии платежных карт; подразумевается комплексный подход к обеспечению информационной безопасности данных платежных карт.

Рис. 1. Нормативы и стандарты по обеспечению кибербезопасности ТЭБ [6]
(Fig. 1. Regulations and standards for cybersecurity of electronic banking technologies [6])

Стандарты Центробанка России «СТО/РС БР ИББС», описывающие методологию обеспечения информационной безопасности, могут быть дополнены рекомендациями и

положениями по управлению кибербезопасностью, содержащимися в международных стандартах ISO/IEC (комплексы 270xx и 2910x), которые направлены на решение определенной задачи управления информационной безопасностью коммерческого банка.

Набор взаимодополняющих документов PCI DSS (Payment Card Industry Data Security Standard, Стандарт безопасности данных индустрии платежных карт) создан компетентными органами международных платежных систем Visa, MasterCard, American Express, JCB и Discover. Стандарты PCI DSS являются совокупностью из двенадцати детализированных требований обеспечения информационной безопасности держателей платежных карт (с учетом передачи, хранения и обработки этих карт в информационных инфраструктурах организаций).

Набор единых требований, стандартов и методик регулирования банковского дела, которые принимаются в различных странах, разрабатывается Базельским комитетом по банковскому надзору (БКБН). Эта организация действует при Банке международных расчетов. Совершенствованию банковского надзора посвящены документы Basel II, а также Basel III и Basel IV [6]. С их содержанием, а также со статьями ведущих экспертов в области банковского надзора можно познакомиться на сайте БКБН <https://www.bis.org>.

В [4–5] рассматриваются документы Basel II при наличии Basel III и IV. Причина в том, что внедрение итогового набора регуляторных требований к банкам, включающего в себя все изменения Базеля III и пересмотренные подходы к оценке рыночного риска, первоначально планировавшееся на 2019 г., теперь перенесено на 2022 г. Банк России собирается внедрить соответствующие изменения в регулирование кредитно-финансовой деятельности Российской Федерации, в т.ч. в части регулирования рыночного риска, в сроки, предусмотренные БКБН². Пандемия COVID-19, возможно, затормозит развитие. О внедрении Базель IV речь вообще не идет.

Поскольку банковская отрасль чрезвычайно консервативна и нередко инертна [1], то любые нововведения должны быть очень аккуратны. В работе [7], посвященной реинжинирингу, наряду с методическими указаниями, приведены примеры (кейсы) фундаментальной переработки и радикальной перестройки бизнес-процессов для того, чтобы получить максимальный эффект от производственно-хозяйственной и финансово-экономической деятельности. Предложена модель РЕММ, позволяющая оценить стадии развития сложных процессов компании, по 9 направлениям:

1. Проектирование сквозного (межфункционального) процесса;
2. Исполнители бизнес-процесса;
3. Компетенции руководителя процесса;
4. Инфраструктура (информационная система);
5. Определение и использование показателей результата деятельности;
6. Представители высшего руководства;
7. Качество обслуживания и культура работы предприятия;
8. Специалисты в области перестройки и реализации процессов;
9. Структура управления процессами.

Таким образом, модель РЕММ позволяет определить стадию развития внедряемого бизнес-процесса и увидеть, какое направление должно быть улучшено или доработано [7]. Методология реинжиниринга, используемая с 1990 г., имеет значительные преимущества, такие как снижение затрат и рост производительности, улучшение качества продукции и повышение удовлетворенности клиентов [8]. Схема взаимодействий при реализации РВКа в кредитной организации (инцидента информационной безопасности) представлена на рис. 2.

---

²См. подробнее о сроках внедрения Базеля III: URL: https://cbr.ru/press/pr/?file=06022018_120000ik2018-02-06t11_55_45.htm (дата обращения: 24.11.2020).

Схема иллюстрирует переход от децентрализованной (местные SOC) к централизованной (государственные CERT и CSIRT) системе управления РВКа в ТЭБ.

*Рис. 2. Схема взаимодействий при реализации РВКа в банке
(Fig. 2. Scheme of interactions in the risk of cyberattacks in a bank)*

Таким образом, основа для доверительного отношения клиентов и контрагентов банка к его продуктам формируется благодаря использованию общепризнанных лучших практик, получивших отражение в основных стандартах и требованиях к реализации деятельности организации [6]. Тем не менее, развитие цифровых финансовых технологий требует внедрения новых межфункциональных бизнес-процессов.

2. Разработка метода оценки деятельности киберпреступников

Проанализируем справочные данные о развитии информационного потенциала разных стран, где основной его количественной характеристикой выбран интегральный показатель «Индекс развития электронного правительства»³ (табл. 1 и рис. 3).

Неоднородность информационного пространства имеет тенденцию к возрастанию как на уровне отдельного пользователя и бизнеса, так и на уровне суверенных государств [9], что видно из столбцов «Прирост показателя ВВП» и «Прирост индекса E-gov» таблицы. Это становится причиной возникновения очередных вызовов международной (информационной) безопасности.

Коэффициенты корреляции в первом случае 0,78; во втором случае 0,66. Данные подтверждают, что гаджеты перестали быть признаком роскоши и прочнее вошли в нашу жизнь. Рассматриваемая неоднородность говорит нам о том, что качество услуг ТЭБ и удобство программного продукта (см. введение, п. 2) – параметры относительные и они зависят как от производителя, так и от нарушителей кибербезопасности.

Внедрение новых бизнес-процессов в рамках реинжиниринга содержит разработку новой системы показателей для измерения результата деятельности (англ. Key Performance

³Рейтинг стран мира по индексу развития электронного правительства. URL: <https://gtmarket.ru/ratings/e-government-development-index> (дата обращения: 10.01.2021).

Indicators, KPI) компании, потому что инструменты, которые используются в большинстве компаний для измерения и улучшения производительности, малоэффективны [7] и их эффективность снижается со временем и цифровизацией. В [5] автор определил формулу для оценки резервируемого капитала, который выделяется под киберриск в составе операционного риска банка:

$$R_{\text{РВКа}} = \alpha \cdot \frac{1}{3} \cdot \sum_{i=1}^3 \text{ВД}_i \Big/ \frac{n \cdot IQ_{\text{ЗЛ}} \cdot r}{(d + v) \cdot t}, \quad (1)$$

где числитель $K_{\text{Ор}} = \alpha \cdot \frac{1}{3} \cdot \sum_{i=1}^3 \text{ВД}_i$ задает размер капитала, который выделяется на покрытие операционных рисков в коммерческом банке методом базового индикатора (см. подробнее соглашение БКБН – Basel II). В знаменателе дроби – оценка эффективности кибероружия⁴ ($ef = \frac{n \cdot IQ_{\text{ЗЛ}} \cdot r}{(d + v) \cdot t}$, безразмерная величина). Однако данная формула может

быть применена для определения размера штрафа, выносимого киберпреступникам.

Приведем пример расчета для следующих данных:

- размер капитала, который резервируется в кредитной организации на покрытие операционного риска равен $K_{\text{Ор}} = 10\,000\,000$ руб.
- средний размер ущерба от одной реализации РВКа в ТЭБ, – $n = 11\,000\,000$ руб⁵.
- коэффициент интеллекта киберпреступников, привлеченных к ответственности, чаще всего лежит в интервале 70–90, согласно [10]. Поэтому возьмем $IQ_{\text{ЗЛ}} = 80$ ⁶.
- восстановление непрерывности банковской деятельности (равно времени остановки бизнеса) после реализации РВКа заняло $r = 4$ часа.
- услуги хакеров и расходы на оборудование оценим в $d + v = 500\,000$ руб.
- время изготовления кибероружия $t = 8 \text{ дн.} \times 9 \text{ ч.} = 72$ часа.

Результат вычислений $R_{\text{РВКа}} = 102\,272,7$ руб. получен подстановкой рассмотренных значений в формулу (1) и может представлять размер штрафа, который налагается на компьютерных преступников. Актуальность формулы возросла, когда в ноябре 2020 г. власти России внесли в Государственную Думу законопроект о введении штрафов за нарушение информационной безопасности объектов критической информационной инфраструктуры страны⁷.

---

⁴Обобщенный термин, предлагаемый автором, включает комплекс мер, направленных на осуществление кибератаки и реализацию РВКа.

⁵Лаборатория Касперского подсчитала средний ущерб от кибератаки на бизнес. URL: <https://ria.ru/20160915/1477053600.html> (дата обращения: 20.12.2020).

⁶Деанонимизацией (установлением личности в сети) занимается форензика. Действия в Интернете регистрируются на Web-серверах в специальных журналах, а записи с камер видеонаблюдения, установленных в общественных местах, будут подтверждением действий. Это используется при проведении следственных мероприятий.

⁷Нарушение IT-безопасности КИИ в РФ может грозить штрафом до 500 тыс. рублей. URL: <https://www.securitylab.ru/news/513744.php> (дата обращения: 23.11.2020).

Таблица 1. Динамика развития стран мира по готовности перехода к электронному правительству в зависимости от ВВП на душу населения

Наиболее развитые страны мира	ВВП на душу населения, 2002 (долл.)	Индекс готовности перехода к E-gov, 2004	ВВП на душу населения, 2019 (долл.)	Индекс готовности перехода к E-gov, 2020	Прирост показателя ВВП	Прирост индекса E-gov
Швейцария	40680,0	0,75	70989,0	0,8907	74,51%	18,76%
Соединенные Штаты Америки	37870,0	0,91	65281,0	0,9297	72,38%	2,16%
Япония	34180,0	0,73	43236,0	0,8989	26,50%	23,14%
Дания	33570,0	0,90	59830,0	0,9758	78,22%	8,42%
Исландия	30910,0	0,77	60061,0	0,9101	94,31%	18,19%
Швеция	28910,0	0,87	55815,0	0,9365	93,06%	7,64%
Великобритания	28320,0	0,89	48710,0	0,9358	72,00%	5,15%
Финляндия	27060,0	0,82	51324,0	0,9452	89,67%	15,27%
Австрия	26810,0	0,75	59111,0	0,8914	120,48%	18,85%
Нидерланды	26230,0	0,80	59687,0	0,9228	127,55%	15,35%
Бельгия	25760,0	0,75	54545,0	0,8047	111,74%	7,29%
Германия	25270,0	0,79	56052,0	0,8524	121,81%	7,90%
Франция	24730,0	0,67	49435,0	0,8718	99,90%	30,12%
Канада	24470,0	0,84	51342,0	0,8420	109,82%	0,24%
Австралия	21950,0	0,84	53320,0	0,9432	142,92%	12,29%
Италия	21570,0	0,66	44197,0	0,8231	104,90%	24,71%
Сингапур	21230,0	0,83	101376,0	0,9150	377,51%	9,71%
Республика Корея	12030,0	0,86	43029,0	0,9560	257,68%	11,49%
Россия	2610,0	0,50	29181,0	0,8244	1018,05%	64,88%
Румыния	2260,0	0,55	32297,0	0,7605	1329,07%	38,27%
Китай	1100,0	0,44	16785,0	0,7948	1425,91%	82,46%
Индия	540,0	0,39	7034,0	0,5964	1202,59%	53,75%

Рис. 3. Индекс готовности перехода к электронному правительству в зависимости от ВВП на душу населения (по странам) на начало 2000-х и конец 2010-х гг.
(Fig. 3. Index of readiness for the transition to e-government, depending on GNP per capita (by country) at the beginning of the 2000s and the end of the 2010s)

3. Метод скоростной печати на клавиатуре как организационно-технический бизнес-процесс повышения производительности труда

Реинжиниринг бизнес-процессов и уровень внедрения в компании корпоративной информационной системы (чем и являются ТЭБ) – это различные процессы, которые не должны совмещаться. Если проводится реинжиниринг, то технологии, автоматизирующие процесс, должны «накладываться» только на правильно построенный сквозной бизнес-процесс. Поэтому в данной статье предложено изменение процесса, который проходит через все функции компании, добавляющие ценность продукту, и направлен на работу персонала и клиентов *с уже имеющимися* технологиями. Данный бизнес-процесс назовем методом скоростной печати (МСП) – тема, смежная с информационной безопасностью. Научный результат включает многолетний опыт автора статьи и его эмпирические наблюдения за служащими и клиентами банковских, риэлторских и других офисов, подтвержденные статистикой.

Группа ученых из Aalto University в Финляндии проанализировала технику набора текста на клавиатуре 168 тыс. человек из 200 стран мира и обнаружила, что пользователи, которые набирают текст быстрее, допускают меньше ошибок, а пользователи, которые печатают медленнее, тратят больше времени на поиск и исправление опечаток⁸.

За рубежом МСП – часть школьной программы. В Европе десятипальцевой печатью владеет большинство специалистов «офисных» профессий [11]. Свыше 70% американцев печатают вслепую; в России менее 10% таких людей [12]. Автору удалось связаться с первой и единственной советской чемпионкой по скоростному набору текста на компьютере Элеонорой Алексеевной Лукиной. По ее словам, в Чехии серьезное обучение слепой печати включено в программы почти 100% средних школ и насчет взрослых людей тоже не менее серьезно: от поступающих на государственную службу требуется скорость в МСП не менее 400 зн./мин. Это достигнуто усилиями Ярослава Завьячича и чешской Interinfo (Interinfo – национальное отделение общества Intersteno⁹).

Согласно работам классиков, мозг человека эволюционировал от систематического ручного труда [13]. МСП аналогичен соблюдению правил дорожного движения, без чего на автодороге был бы хаос. Создавая эффект «лежачего полицейского», МСП затормаживает бессознательное движение пользователя вперед при наборе текста, благодаря чему позволяет существенно повысить производительность труда. В музыке порядок расположения и последовательность чередования пальцев рук при игре на музыкальных инструментах называется аппликатурой (от нем. Applikatur и лат. applico – прикладываю, прижимаю). Правильное расположение пальцев – это важный составной элемент мастерства исполнителя. Поэтому аппликатуре уделяется особое внимание (автор знаком с этим на собственном опыте, т.к. осваивал игру на баяне в музыкальной школе).

Навык МСП так же элементарен, как дезинфекция рук врача перед хирургической операцией. Сейчас необходимость дезинфекции рук является аксиомой, но 175 лет назад это невежество приводило к смертям от послеродового сепсиса, вызванного невидимыми частицами (бактериями) на руках хирурга [14].

Благодаря МСП достигается *непрерывность печатания*. Пользователю не приходится искать нужную клавишу и палец, которым ее нажать, – это происходит автоматически. Именно на непрерывности базируется японская методика «Кайдзен»

---

⁸Электронный журнал “Naked Science”. Ученые сформулировали новые правила скоростного набора текста. URL: <https://naked-science.ru/article/sci/uchenye-sformulirovali-novye-pravila> (дата обращения: 22.11.2020).

⁹International Federation for Information and Communication Processing – профессиональное некоммерческое сообщество, направленное на развитие мировых достижений в области технического обеспечения информационного процесса (см. подробнее: intersteno.ru и intersteno.org).

(яп. 改善), направленная на улучшение бизнес-процессов предприятия, а также всех аспектов деятельности. Непрерывность производственного процесса подразумевает ликвидацию незапланированных остановок и задержек в работе, что является достаточным основанием для роста производительности труда (в том числе в кредитно-финансовой деятельности).

Для самостоятельного овладения МСП можно обойтись и без платных тренажеров. В 2009 г. автором статьи был разработан тренажер, который приведен на рис. 4 и устанавливается на рабочий стол монитора. Выровняв текстовый редактор так, как показано на рис. 4., пользователю достаточно набирать любой текст, ориентируясь на мышечную память, сразу «вслепую».

*Рис. 4. Тренажер МСП для самостоятельного освоения
(Fig. 4. High-speed printing simulator for self-development)*

Для разминки между занятиями МСП может использоваться кистевой эспандер – резиновый тор умеренной жесткости. Кроме того, гимнастика для глаз также полезна для восстановления кровоснабжения в глазных мышцах. Упоминание о кистевом эспандере здесь обусловлено II законом Ньютона в импульсном виде:

$$\vec{F} = m \cdot \frac{d\vec{v}}{dt} \Leftrightarrow d\vec{v} = \frac{\vec{F} \cdot dt}{m},$$

где $\vec{F}$ – прилагаемая одиночная сила; m – масса тела; dt – изменение времени движения. При этом изменение скорости $d\vec{v}$ прямо пропорционально прилагаемой силе.

МСП не решит всех проблем информационной безопасности, но позволит избежать ряда незначительных ошибок, которые в совокупности могут дать катастрофическую реализацию РВКа (заметить скрытую переадресацию браузера на мошеннический сайт легче, глядя в монитор при наборе текста). Более того, МСП может стать одним из биометрических признаков клиента (например, работы [15–16] посвящены анализу

функционального динамического комплекса навыков пользователя для воспроизведения аутентифицирующего жеста) – тема для дальнейших исследований.

МСП на клавиатуре предлагается ввести в образовательную программу России для развития мышечной памяти пользователя и повышения его киберграмотности [11, 12, 17]. Практическая целесообразность освоения МСП в школе обусловлена тем, что в повседневной деятельности человек должен обладать навыком по информатике, который имеет прикладное значение в реальной жизни¹⁰.

Освоение МСП на уроках информатики будет способствовать развитию физических умений обращения с компьютером наряду с улучшением интеллектуальных качеств, а это, в свою очередь, – укреплению киберграмотности и компьютерной дисциплины. Следующий шаг после освоения МСП – соревнования на сайтах, подобных <http://klavogonki.ru/> (клавиатурный тренажер в игровой форме).

Заключение

Соответствие коммерческого банка – участника финансовой системы передовым практикам и/или общепризнанным известным стандартам, которые проверены временем и имеют независимую оценку (аудит), является основой для доверия его контрагентов и клиентов к финансовым технологиям этого банка.

Неоднородность киберпространства порождает нестабильность качества услуг ТЭБ и удобства программного продукта. Одна из причин неоднородности – компьютерная преступность. В статье предложена оценка для определения штрафа за нарушение защиты критической информационной инфраструктуры.

Проанализирована скоростная печать на клавиатуре как межфункциональный бизнес-процесс, который будет способствовать увеличению производительности и дохода кредитной организации за счет уменьшения доли затрат и количества операционных ошибок, порождаемых непредусмотренными прерываниями при наборе текста (уровень финансовой и компьютерной грамотности клиента и специалиста банка).

СПИСОК ЛИТЕРАТУРЫ:

1. King B. Bank 4.0: Banking Everywhere, Never at a Bank. Singapore: John Wiley & Sons Limited, 2018. – 352 p.
2. Skinner C. Digital Human: The Fourth Revolution of Humanity Includes Everyone. Singapore: Marshall Cavendish International (Asia), 2018. – 328 p.
3. Пospelов А.Л., Ревенков П.В. Что сдерживает использование дистанционных каналов обслуживания? // Расчеты и операционная работа в коммерческом банке. 2015. № 1 (125). С. 70–75. URL: http://www.reglament.net/bank/raschet/2015_1/get_article.htm?id=3823 (дата обращения: 18.12.2020).
4. Бердюгин А.А., Ревенков П.В. Оценка риска воздействия кибератак в технологиях электронного банкинга (пример программной реализации) // Финансы: теория и практика. 2020. Т. 24, № 6. С. 51–60. DOI: <http://dx.doi.org/10.26794/2587-5671-2020-24-6-51-60>.
5. Ревенков П.В., Бердюгин А.А. Метод количественной оценки риска воздействия кибератак в условиях электронного банкинга // Банковское дело. 2020. №7. С. 32–37.
6. Воронин А.С. Национальная платежная система. Бизнес-энциклопедия. М.: КНОРУС: ЦИПСИР, 2013. – 424 с.
7. Хаммер Майкл, Лиза Хершман. Быстрее, лучше, дешевле: Девять методов реинжиниринга бизнес-процессов. М.: Альпина Паблишер, 2017. – 352 с.
8. Mahmoud AbdEllatif, Marwa Salah Farhan, Naglaa Saeed Shehata. Overcoming business process reengineering obstacles using ontology-based knowledge map methodology. Future Computing and Informatics Journal. 2018. V. 3, Iss. 1, P. 7–28. DOI: <https://doi.org/10.1016/j.fcij.2017.10.006>.

---

¹⁰См. подробнее № 25 еженедельника «Аргументы и Факты», статья «Почему задания ЕГЭ по математике такие простые?». URL: https://aif.ru/dontknows/actual/pochemu_zadaniya_ege_po_matematike_takie_prostyie (дата обращения: 08.12.2020).

9. Роговский Е.А. Кибер-Вашингтон: глобальные амбиции. М.: Международные отношения, 2014. – 848 с.
10. Arthur Jensen. The g Factor: The Science of Mental Ability. Greenwood Publishing Group, Inc. (GPG), Santa Barbara, California, 1998. – 648 p.
11. Ильнер А.О. Подготовка переводчиков в России и за рубежом: сравнительный анализ // Образование и наука. 2010. № 8 (76). С. 65–70. URL: <https://cyberleninka.ru/article/n/podgotovka-perevodchikov-v-rossii-i-za-rubezhom-sravnitelnyy-analiz> (дата обращения: 11.12.2020).
12. Шахиджян В.В. Готов научить всех // Авиасалоны мира. 2007. № 2. С. 46–47. URL: https://issuu.com/dizone/docs/aviasalony_all_2007_mini (дата обращения: 11.12.2020).
13. Лобанов В.В. Роль труда в опытах физического воспитания В.С. Пирусского // Вестник Томского государственного педагогического университета. 2013. № 9 (137). С. 181–187. URL: <https://www.elibrary.ru/item.asp?id=20933711> (дата обращения: 12.12.2020).
14. Newsom S. W. B. Ignaz Philipp Semmelweis. Journal of Hospital Infection. 1993. V. 23, Iss. 3. P. 175–187. URL: <https://sciencedirect.com/science/article/abs/pii/019567019390023S> (дата обращения: 10.12.2020).
15. Козлов Ю.Е. Использование методов визуальной аналитики для получения комплексного показателя качества биометрической аутентификации с использованием механизма жестовой манипуляции // Научная визуализация. 2019. Т. 11. № 2. С. 99–113. URL: <http://sv-journal.org/2019-2/08/> (дата обращения: 18.12.2020). DOI: <http://dx.doi.org/10.26583/sv.11.2.08>.
16. Береснева, Анастасия В.; Елишкина, Анна В. Подходы к онлайн верификации собственноручной подписи. Безопасность информационных технологий, [S.l.]. Т. 27, № 2. С. 78–85, июнь 2020. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1272>. (дата обращения: 18.12.2020). DOI: <http://dx.doi.org/10.26583/bit.2020.2.06>.
17. Андреев А.Н., Румянцев С.А. Особенности подготовки специалистов в сфере информационных технологий и использование компьютерных программ с целью повышения качества самообразования // Труды международного симпозиума «Надежность и качество». 2012. Т. 1. С. 388–391. URL: <https://noosphere.ru/pubs/344211> (дата обращения: 18.12.2020).

REFERENCES:

- [1] King B. Bank 4.0: Banking Everywhere, Never at a Bank. Singapore: John Wiley & Sons Limited, 2018. – 352 p.
- [2] Skinner C. Digital Human: The Fourth Revolution of Humanity Includes Everyone. Singapore: Marshall Cavendish International (Asia), 2018. – 328 p.
- [3] Pospelov A.L., Revenkov P.V. What hinders the use of remote service channels? Calculations and operational work in a commercial Bank. 2015, no. 1 (125). P. 70–75 URL: http://www.reglament.net/bank/raschet/2015_1/get_article.htm?id=3823 (accessed: 18.12.2020) (in Russian).
- [4] Berdyugin A.A., Revenkov P.V. Cyberattack risk assessment in electronic banking technologies (the case of software implementation). Finance: Theory and Practice. 2020. V. 24, no. 6. P. 51–60. DOI: <http://dx.doi.org/10.26794/2587-5671-2020-24-6-51-60>. (in Russian)
- [5] Revenkov P.V., Berdyugin A.A. Method of quantifying the risk of cyberattacks in the context of electronic banking. Bankovskoye delo = Banking. 2020, no. 7. P. 32–37 (in Russian).
- [6] Voronin A.S. National payment system. Business encyclopedia, Moscow: KNORUS: Tsipsir, 2013. – 424 p.
- [7] Hammer M., Hershman L. Faster Cheaper Better: The 9 Levers for Transforming How Work Gets Done. Moscow, Alpina Publisher, 2017. – 352 p.
- [8] Mahmoud Abdellatif, Marwa Salah Farhan, Naglaa Saeed Shehata. Overcoming business process reengineering obstacles using ontology-based knowledge map methodology. Future Computing and Informatics Journal. 2018. V. 3, Iss. 1, P. 7–28. DOI: <https://doi.org/10.1016/j.fcij.2017.10.006>.
- [9] Rogovsky E.A. Cyber-Washington: global ambitions. Moscow: International relations; 2014. – 848 p. (in Russian).
- [10] Arthur Jensen. The g Factor: The Science of Mental Ability. Greenwood Publishing Group, Inc. (GPG), Santa Barbara, California, 1998. – 648 p.
- [11] Ilnier A.O. The analysis of training translators and interpreters in Russia and abroad. Education and Science. 2010, no. 8 (76). P. 65–70. URL: <https://cyberleninka.ru/article/n/podgotovka-perevodchikov-v-rossii-i-za-rubezhom-sravnitelnyy-analiz> (accessed: 11.12.2020) (in Russian).
- [12] Shakhidjanyan V.V. Ready to teach everyone. Airshows of the world. 2007, no. 2. 46–47. URL: https://issuu.com/dizone/docs/aviasalony_all_2007_mini (accessed: 11.12.2020) (in Russian).
- [13] Lobanov V.V. The role of craft in the physical education practices by V.S. Pirusky. Bulletin of the Tomsk State Pedagogical University. 2013, no. 9 (137). P. 181–187. URL: <https://www.elibrary.ru/item.asp?id=20933711>. (accessed: 12.12.2020) (in Russian).

- [14] Newsom S. W. B. Ignaz Philipp Semmelweis. Journal of Hospital Infection. 1993. V. 23, Iss. 3. P. 175–187. URL: <https://sciencedirect.com/science/article/abs/pii/019567019390023S> (accessed: 10.12.2020)
- [15] Kozlov Yu.E. Use of methods of visual analytics to obtain integrated indicator of the quality of biometric authentication using the mechanism gesture manipulation. Scientific Visualization, 2019. V. 11, no. 2. P. 99–113. URL: <http://sv-journal.org/2019-2/08/> (accessed: 18.12.2020). DOI: <https://doi.org/10.26583/sv.11.2.08>.
- [16] Beresneva, Anastasia V., Epishkina, AnnaV. Approaches to online handwritten signature verification. IT Security (Russia), [S.l.]. V. 27, no. 2. P. 78–85, June 2020. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1272>. (accessed: 18.12.2020). DOI: <http://dx.doi.org/10.26583/bit.2020.2.06>.
- [17] Andreev A.N., Rumyantsev S.A. Features of training specialists in the field of information technologies and the use of computer programs to improve the quality of self-education. Proceedings of the international Symposium “Reliability and quality”, 2012. V. 1. P. 388–391. URL: <https://noosphere.ru/pubs/344211> (in Russian).

*Поступила в редакцию – 19 декабря 2020 г. Окончательный вариант – 01.02.2021 г.
Received – December 19, 2020. The final version – February 01, 2021.*