2) наблюдение, анкетирование, интервью, анализ документов, результатов работы и опыта конкретного сотрудника [7, с. 207].

В связи с вышеизложенным, можно сделать вывод о целесообразности использования социологического метода исследования в системе управления персоналом. В современной литературе существует множество методов данного исследования, которая открывает возможности применения и анализа социальных явлений, происходящих в коллективе. Данный метод исследования оказывает существенное влияние на эффективность управленческой деятельности: позволяет ознакомить руководителя с нынешней и будущей ситуацией в коллективе, также позволяет руководителю влиять на сотрудников и управлять ими, обеспечивает процесс информатизации и информационной безопасности. Именно благодаря перечисленным методикам современный руководитель фирмы может делать реальные прогнозы развития качества работы сотрудников, которая даст ему возможность получения необходимого социального эффекта.

Библиографические ссылки

1. Александрова А. А., Ерёмина К. Е. Социологические исследования в системе управления персоналом // В сборнике : Традиционное, современное и переходное в условиях модернизации Российского общества. 2018. С. 12–14.
2. Жидкова М. С. Использование социологических методов в управленческой работе менеджера (теоретический аспект) // В сборнике : Развитие современных инновационных технологий и методик в образовательных учреждениях. 2021. С. 165–169.
3. Мунич Д. О. Социально-психологические методы управления в системе методов управления социально-экономическими системами // Студенческий форум. 2020. № 40-3 (133). С. 30–32.
4. Мунич Д. О. Социально-психологические методы управления // Студенческий форум. 2021. № 20-2 (156). С. 83–85.
5. Кириллова В. Э., Закирова А. Р. Особенности применения методов социологических исследований // Казанский педагогический журнал. 2018. № 3 (128). С. 199–203.
6. Королева А. С. Социологические исследования в системе управления персоналом // В сборнике : Традиционные, современные и переходные в условиях модернизации российского общества. 2018. С. 74–77.
7. Крамская К. А. Психолого-социологические методы повышения результативности кадрового потенциала в управлении персоналом организации // В сборнике : Институты и механизмы инновационного развития: мировой опыт и российская практика. 2019. С. 206–210.
8. Рожнова А. Р. Социаологические методы в кадровых процессах // В сборнике : Качество жизни населения в современном российском обществе: социокультурные и социально-экономические аспекты. 2020. С. 118–121.
9. Сушкова Е. В. Моделирование социологического обеспечения управления в организации // Труд и социальные отношения. 2019. № 2. С. 159–168.

УДК 321.8; 338.23

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ФИНАНСОВОГО СЕКТОРА И ЕЕ КАДРОВОЕ РЕШЕНИЕ

А. М. Белобородько

доцент, Московский экономический институт, Москва, Российская Федерация, alex_belob@mail.ru

Настоящая статья посвящена одной из наиболее злободневных проблем современной цифровой экономики – ее информационной безопасности. В большей степени это касается финансового сектора, осуществляющего электронные транзакции и активно ищущего

сегодня более эффективные аналоги металлических монет, бумажных банкнот, пластиковых карт и пр. Основной причиной указанных проблем, по всей видимости, следует назвать острый дефицит специалистов, владеющих современными информационными технологиями и понимающих суть происходящих изменений, связанных с цифровизацией экономики.

Ключевые слова: цифровая экономика; информационная безопасность; финансовый сектор; кадровое обеспечение.

INFORMATION SECURITY OF THE FINANCIAL SECTOR AND ITS HUMAN RESOURCES

A. M. Beloborodko

Associate Professor, Moscow Economic Institute, Moscow, Russian Federation, alex_belob@mail.ru

This article is devoted to one of the most pressing problems of the modern digital economy – its information security. To a large extent, this concerns the financial sector, which carries out electronic transactions and is actively looking for more efficient analogues of metal coins, paper banknotes, plastic cards, etc. The main reason for these problems, most likely, should be called an acute shortage of specialists in the field of modern information technologies and who understand the essence of the ongoing changes associated with the digitalization of the economy.

Keywords: digital economy; information security; financial sector; human resources

В настоящее время цифровизация экономики является объективной реальностью. С наступлением информационного общества система социальных отношений претерпевает весьма существенные изменения [1]. Развитие информационных технологий в контексте NBIC-конвергенции и развертывания шестого технологического уклада неминуемо приводит к автоматизации и роботизации широкого ряда трудовых функций, весь жизненный уклад, быт зависят теперь от интенсивного ускорения движения информации [2].

Сегодня под цифровой экономикой в «Стратегии развития информационного общества РФ на 2017–2030 годы» понимается «хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг» [3]. Изучением политэкономического феномена цифровой экономики занимались, начиная с 1995 года отечественные и зарубежные исследователи, в числе которых Н. Негропонте (автор термина), Е. Н. Ведута, Л. П. Гончаренко, С. Ю. Глазьев, А. И. Гретченко, В. В. Иванов, М. Йоль, Г. Кайдзюн, М. В. Кудина, В. И. Маевский, Г. Г. Малинецкий, Д. Тапскотт, А. Эспиноса и др. [4].

Анализ действующей нормативно-правовой базы, публичных заявлений официальных лиц, экспертных оценок, опросов общественного мнения и федеральных проектов и программ выявил большую потребность в кадрах, способных обеспечить современный финансовый сектор российской экономики необходимым уровнем информационной безопасности.

В настоящее время, по данным Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации [5], в России в контексте реализации Указа Президента РФ от 7 мая 2018 г № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» в условиях необходимости обеспечения ускоренного внедрения цифровых технологий в экономике и социальной сфере, Правительство РФ разработало и внедряет национальную

программу «Цифровая экономика Российской Федерации», утвержденную протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7 и нацеленную на увеличение внутренних затрат на развитие цифровой экономики за счет всех источников; создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств; использование преимущественно отечественного программного обеспечения государственными органами, органами местного самоуправления и организациями. Указанные в паспорте национальной программы цели, как очевидно, не отражают в полной мере проблему кадрового обеспечения информационной безопасности финансового сектора российской экономики.

В структуру национального проекта входит шесть федеральных проектов, в числе которых «Нормативное регулирование цифровой среды»; «Информационная инфраструктура»; «Кадры для цифровой экономики»; «Информационная безопасность»; «Цифровые технологии» и «Цифровое государственное управление». Два проекта из шести указывают на актуальность и важность рассматриваемой нами проблемы, а также подчеркивают факт проявления внимания руководством страны к решению указанных вопросов.

Хотя Федеральный проект «Информационная безопасность» нацелен на решение вопросов, связанных с обеспечением информационной безопасности на основе отечественных разработок, по мнению автора этой статьи, эффект от реализации нацпрограммы, будет трудно заметен, поскольку возникают вопросы, связанные с неполной реализацией вложенных в программу бюджетных средств и с отсутствием единой стратегии информационной безопасности на юридическом уровне, и какова она вообще.

Создавшаяся ситуация наглядно иллюстрирует отсутствие детальной проработки вопросов информационной безопасности финансового сектора экономики РФ, указывая на отсутствие профилактических мер по предотвращению противоправных действий в этой сфере.

Федеральный проект «Кадры для цифровой экономики» нацелен на «обеспечение подготовки высококвалифицированных кадров для цифровой экономики». Как показывает анализ паспорта национального проекта вопрос о кадровом обеспечении информационной безопасности финансового сектора российской экономики остается открытым. В проекте заявлено 32 позиции, деликатно обходящие данный вопрос, имеющий, очевидно, для информационной безопасности финансового рынка РФ первостепенное значение.

В 2018 году был принят очень важный документ «ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», знание и руководство которым, по мнению автора статьи, необходимо практически любому работнику финансовой сферы. Однако следует констатировать, что профессиональные стандарты, являющиеся своего рода выражением спроса работодателей на рабочую силу, были разработаны и приняты несколько раньше, поэтому вопрос о компетентности сотрудников финансовой сферы в области информационной, цифровой безопасности там не нашел должного отражения. Так, например, в профессиональных стандартах специалиста по платежным системам (зарегистрирован в Минюсте России 23 апреля 2015 г. N 37025); специалиста по платежным услугам (зарегистрирован в Минюсте России 24 ноября 2016 г. N 44419); специалиста по дистанционному банковскому обслуживанию (зарегистрирован в Минюсте России 11 мая 2017 г. N 46685) и др. никакие

существенные аспекты обеспечения информационной безопасности в трудовых функциях указанных сотрудников не отражены. Между тем, бизнес-сообщество крайне обеспокоено данными вопросами. Так, в частности, Совет ТПП РФ по финансово-промышленной и инвестиционной политике в этом году (02.06.2020 г.) провел вебинар для представителей предпринимательского сообщества и торгово-промышленных палат по теме «Информационная безопасность для финансовых организаций», подобные вебинары нередко проводя ведущие вузы страны (РАНХиГС при президенте РФ, Финансовый университет при Правительстве РФ, Российский экономический университет имени Г. В. Плеханова и др.). Вопрос об обеспечении информационной безопасности стоит очень остро не только внутри страны, но и на международном уровне. Так 25 сентября 2020 года президент РФ В.В. Путин выступил с заявлением о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности [3].

Ключевой проблемой обеспечения информационной безопасности финансового сектора, тормозящей полноценный, быстрый и безболезненный переход к цифровой экономике, является несоответствие спроса финансовых организаций на кадры предложениям рынка труда. Важно отметить, что в Атласе новых профессий 3.0, разработанных Сколково и Агентством стратегических инициатив, указана профессия «Аналитик кибербезопасности в финансовом секторе» [6], который будет специализироваться на анализе и поиске оптимальных решений по минимизации рисков, связанных с автоматизацией управления личными финансами, межмашинными транзакциями и облачными решениями, а также будет обладать навыками выявления уязвимости в смарт-контрактах [7].

Вероятно, наряду с профессией аналитика кибербезопасности в финансовом секторе понадобятся разработчики, производители и администраторы систем информационной безопасности, а также промоутеры цифровой финансовой грамотности населения. Потребуется внести соответствующие изменения в действующее законодательство, в порядок работы органов государственной власти, производственных предприятий, финансовых и некоммерческих организаций, поэтому понадобятся юристы и государственные гражданские служащие, специализирующиеся на данных вопросах. Очевидно, что должны появиться соответственные образовательные программы высшего и среднего профессионального образования. Существующие федеральные государственные образовательные стандарты ориентированы исключительно на подготовку технических специалистов, что указывает на системный разрыв между потребностями рынка труда и возможностями системы образования.

По всей видимости, проблему информационной безопасности финансового сектора требуется решать комплексно [8, 9]. Политическое управление системой кадрового обеспечения информационной безопасности финансового сектора представляется очень важным, если не приоритетным, направлением в деятельности правящей элиты. Общество в условиях декларируемой прозрачности управления нуждается в своевременном и полном понимании протекающих процессов. Глобализация и развитие международного рынка труда приводит к увеличению миграции трудоспособного населения, заинтересованного в модернизации системы электронного документооборота и платежных систем.

Эколого-экономическим фактором, определяющим направление и порядок трансформации кадрового обеспечения информационной безопасности финансового сектора, во многом может выступать появление новой среды обитания – виртуального пространства, отличающегося своими особенностями и подходами к формированию общественных отношений, к решению глобальных проблем современности, к изменению социальных ролей, черт характера и структуры мировоззрения современного человека.

Технологически развитие кадрового обеспечения информационной безопасности финансового сектора будет связано с появлением новой организации общества, структуру которого будут определять архитектора информационной среды, создатели контента, разработчики и администраторы средств массовой коммуникации, высокотехнологического оборудования и наукоемких технологий.

Библиографические ссылки

1. Dufva T., Dufva M. Grasping the future of the digital society, Futures, Volume 107, March 2019, Pages 17–28 : [Электронный ресурс]. URL: https://doi.org/10.1016/j.futures.2018.11.001 (дата доступа: 15.09.2021).
2. Dijck J. Governing digital societies: Private platforms, public values, Computer Law & Security Review, Volume 36, April 2020, 105377. Pages 3–4 : [Электронный ресурс]. URL: https://doi.org/10.1016/j.clsr.2019.-105377 (дата доступа: 01.09.202)1
3. Указ Президента Российской Федерации от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» : [Электронный ресурс]. URL: http://www.kre-mlin.ru/acts/bank/41919 (дата доступа: 01.09.2021).
4. Министерство науки и высшего образования Российской федерации приказ от 9 августа 2019 г. N 590 «Цифровая экономика российской федерации» : [Электронный ресурс]. URL: https://vak.minobrnauki.gov.ru/ (дата доступа: 01.09.2021).
5. Указ президента российской федерации от 7 мая 2018 года № 204 «О национальных целях и стратегических задачах развития российской федерации на период до 2024 года» : [Электронный ресурс]. – URL: https://digital.gov.ru/ (дата доступа: 01.10.2021).
6. Атлас новых профессий 3.0 : [Электронный ресурс]. URL: https://www.skolkovo.ru/ (дата доступа: 01.10.2021).
7. Macnish K., van der Ham J. Ethics in cybersecurity research and practice, Technology in Society, Volume 63, November 2020, 101382 : [Электронный ресурс]. URL: https://doi.org/10.1016/j.techsoc.2020.101382 (дата доступа: 01.10.2021).
8. Chong H.-Y., Diamantopoulos A. Integrating advanced technologies to uphold security of payment: Data flow diagram, Automation in Construction, Volume 114, June 2020, 103158 : [Электронный ресурс]. URL: https://doi.org/10.1016/j.autcon.2020.103158 (дата доступа: 01.09.2021).
9. Ficco M., Palmieri F. Leaf: An open-source cybersecurity training platform for realistic edge-IoT scenarios, Journal of Systems Architecture, Volume 97, August 2019, Pages 107–129 : [Электронный ресурс]. URL: https://doi.org/10.1016/j.sysarc.2019.04.004 (дата доступа: 01.09.2021).

УДК 336

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН В ЭКОНОМИКЕ

Ю. А. Белова[1)], А. В. Матохина[2)], Л. Н. Макарова[3)]

[1)] *студент, Белорусский государственный экономический университет, Минск, Республика Беларусь, black.torn@mail.ru*

[2)] *студент, Белорусский государственный экономический университет, Минск, Республика Беларусь, matokhina-alina@mail.ru*

[3)] *доцент, Белорусский государственный экономический университет, Минск, Республика Беларусь, makarava@tut.by*

В ходе данной работы была исследована технология блокчейн, как перспективный фактор развития мировой экономики. Рассмотрев различные отрасли экономики, такие как банковский и финансовый сектор, логистику, бухгалтерский учет на примере успешных иностранных компаний, мы выделили явные практические преимущества использования данной технологии, описали применение этой технологии в Беларуси, а также возникающие проблемы при ее внедрении.

Ключевые слова: блокчейн; экономика; транзакция; смарт-контракт; криптовалюта.