УДК 351.72:351.746(470+571)

К ВОПРОСАМ ОБ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФИНАНСОВОГО СЕКТОРА РОССИЙСКОЙ ФЕДЕРАЦИИ И НЕОБХОДИМОСТИ РАЗВИТИЯ КАДРОВОГО ПОТЕНЦИАЛА

А.М. Белобородько
канд. экон. наук,
доцент кафедры экономики и управления
НОЧУ ВО «Московский экономический институт» (Москва)

Н.В. Фадейкина
д-р экон. наук, профессор,
Заслуженный деятель науки и Заслуженный экономист Новосибирской области,
профессор кафедры общественных финансов,
ФГБОУ ВО «Новосибирский государственный университет экономики и управления «НИНХ»,
главный редактор научного журнала «Сибирская финансовая школа» (Новосибирск)

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 более эффективные аналоги металлических монет, бумажных банкнот и пр. Основной причиной указанных проблем является острый дефицит специалистов, владеющих современными информационными технологиями и понимающих суть происходящих изменений, связанных с цифровой трансформацией экономических процессов. Рассмотрены пути преодоления кадрового голода и отражения кибератак в финансовых структурах.

Ключевые слова: информационная безопасность, финансовый сектор, цифровая трансформация экономических процессов, кадровое обеспечение.

С наступлением эры информационного общества система социально-экономических отношений претерпела весьма существенные изменения [1]. Цифровая трансформация экономических процессов стала сейчас объективной реальностью. Развитие информационных технологий в контексте NBIC-конвергенции[1] и развертывания шестого технологического уклада неминуемо приводит к автоматизации и роботизации широкого ряда трудовых функций, меняет весь жизненный уклад особенно в условиях пандемии. Наша жизнь в условиях пандемии теперь зависит от интенсивного ускорения движения информации [2] и цифровой трансформации экономических и иных процессов.

Успешная трансформация экономики в новый цифровой формат является необходимым условием конкурентоспособности России на мировом рынке.

Напомним, что в «Стратегии развития информационного общества РФ на 2017–2030 годы»[2] цифровой экономикой названа «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». Политэкономиче-

[1] Термин *NBIC-конвергенция*, характеризующий явление взаимовлияния информационных технологий, биотехнологий, нанотехнологий и когнитивной науки, названный по первым буквам указанных областей (*N* – нано; *B* – био; *I* – инфо; *C* – когно), введен в 2002 г. Михаилом Роко и Уильямом Бейнбриджем, авторами наиболее значительной в этом направлении на данный момент работы – отчета Converging Technologies for Improving Human Performance, подготовленного 2002 г. во Всемирном центре оценки технологий (WTEC). Отчет посвящен раскрытию особенности NBIC-конвергенции, ее значению в общем ходе развития мировой цивилизации, а также ее эволюционному и культурообразующему значению / Прайд В., Медведев Д.А. Феномен NBIC-конвергенции: Реальность и ожидания. URL: http://transhumanism-russia.ru/content/view/498/ (дата обращения: 17.11.2021).

[2] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента Рос. Федерации от 9 мая 2017 г. № 203.

ский феномен цифровой экономики изучали, начиная с 1995 г., зарубежные исследователи, в числе которых Н. Негропонте (автор термина) [3], Д. Тапскотт, Э. Вильямс [4], а также такие отечественные ученые, как С.Ю. Глазьев [5; 6], О.В. Китова [7], М.С. Марамыгин [8], А.И. Новиков [9], А.А. Пороховский [10], Янгиров А.В. [11] и др.

Новый формат дигитальной экономики качественно изменил состояние отечественного человеческого и социального капитала, нашедшего отражение в атласе профессий и новых социальных статусах. В результате анализа существующей нормативно-правовой базы, экспертных оценок, опросов общественного мнения, федеральных проектов и государственных программ выявлена острая потребность в кадрах, необходимых для функционирования современного финансового сектора российской экономики, обеспеченного необходимым уровнем информационной безопасности. Не секрет, что развитие финансового рынка отягощено хакерскими киберугрозами, причем, с каждым годом количество кибератак увеличивается и уровень киберугроз повышается.

В то время как киберпреступность растет экспоненциально, финансовые организации сталкиваются с серьезной нехваткой квалифицированных кадров в области кибербезопасности: квалифицированных специалистов в этой сфере катастрофически не хватает, и конкуренция за их услуги постоянно растет.

С каждым днем количество публикаций о нехватке ИТ-талантов (особенно в Интернет-среде) увеличивается[3]. С точки зрения безопасности бизнеса, отсутствие опытных специалистов в области защиты от киберугруз невероятно опасно. Когнитивные знания и опыт в области кибербезопасности как никогда востребованы, поскольку сейчас во время пандемии специалисты многих компаний работают удаленно, а киберугрозы продолжают расти и становятся все более опасными для современного бизнеса.

В России, начиная с 2019 г., ощущается заметная нехватка передовых навыков кибербезопасности у персонала. Найти опытного аналитика безопасности, исследователя угроз, архитектора безопасности или архитектора облачной безопасности – непростая задача; для заполнения подобных вакансий обычно требуется несколько месяцев поиска, а также значительных инвестиций в человеческий капитал. Помимо проблем, связанных с повышением уровня ИТ-компетентности персонала, компании должны постоянно защищаться от угроз в режиме реального времени, поэтому они вынуждены принимать по найму специалистов в команду по кибербезопасности, работающую в режиме 24×7×365, что значительно усложняет процесс найма, и в первую очередь, из-за высокой стоимости такого специалиста. Киберпреступники не отдыхают по выходным, ночам или даже в канун Рождества, поэтому найти кандидатов на вакансии с рабочим графиком «в любое время суток», в выходные и праздничные дни невероятно сложно на отечественном рынке труда.

На фоне продолжающегося и увеличивающегося роста услуг в сфере облачных вычислений нехватка специалистов по кибербезопасности может привести к катастрофическим последствиям для бизнеса, не имеющего соответствующей киберзащиты.

Период 2020–2021 гг. для финансового рынка России стал самым непростым во многих отношениях. Среди серьезных проблем – киберугрозы во всех отраслях, чему во многом способствует характер транзакционных операций на финансовых рынках. Особенно кибератаки участились в период перевода работников компаний на дистанционный формат работы или увольнения персонала. Большинство финансовых институтов и организаций здравоохранения подверглись серьезным кибератакам, что привело к взломам архивов, проникновению программ-вымогателей и сбоям в работе компаний. И сейчас в период роста интернет-продаж нет никаких признаков ослабления угроз.

Каким же образом киберпреступники превращают ваши данные в наличные? У хакеров есть множество способов «монетизировать» украденные данные, но, как правило, Организованная преступная группа (далее – ОПГ) либо сделает это сама, либо продаст украденные данные другим преступникам для использования в так называемом «вторичном мошенничестве».

Для использования украденных денежных средств с банковских счетов ОПГ, как правило, пользуется услугами специалистов (известных как «денежные мулы» и/или «пастухи мулов») для отмывания украденных денег через множество счетов, в конечном итоге с переводом их за рубеж на оффшорные счета, принадлежащие лидерам ОПГ.

[3] Приведем примеры таких публикаций: *Добровольский Н.* Ускользающий талант: Россия теряет лучших ИТ-специалистов. URL: https://vc.ru/hr/101459-uskolzayushchiy-talant-rossiya-teryaet-luchshih-it-specialistov; *Башкатова А.* Российские айтишники смотрят на Запад. URL: https://www.ng.ru/economics/2021-11-30/1_8314_it.html; *Алпатова И.* Как государство разберется с дефицитом технологичных кадров / Российская газета – Федеральный выпуск № 33 (8384). URL: https://rg.ru/2021/02/16/kak-gosudarstvo-razberetsia-s-deficitom-tehnologichnyh-kadrov.html; *Воронович Г.* Сотни тысяч новых кадров: как в России поддерживают ИТ-сектор. URL: https://www.gazeta.ru/tech/2020/12/04_a_13387279.shtml; *Мотренко Е.* Айтиважно: как решить проблему нехватки специалистов. URL: https://iz.ru/1061536/elena-motrenko/aitivazhno-kak-reshit-problemu-nekhvatki-it-spetcialistov (дата обращения: 23.12.2021).

Есть и другие технологии и «бизнес-модели» у хакеров: они практикуют продажу украденных сведений (данных) через криминальные сайты. Для наиболее организованных и технически продвинутых ОПГ операции по краже денег (сведений) выполняются «внутри собственной компании» посредством использования «инструментария собственных бизнес-моделей». Практики применения бизнес-моделей (онлайн) киберпреступников описаны в публикации Национального центра кибербезопасности[4].

На сайте Лаборатории Касперского[5] даны советы по защите от киберпреступников и приведены несколько примеров различных типов их преступлений, а именно:

- мошенничество с электронной почтой и интернет-мошенничество;
- мошенничество с использованием личных данных (кража и злонамеренное использование личной информации);
- кража финансовых данных или данных банковских карт;
- кража и продажа корпоративных данных;
- кибершантаж (требование денег для предотвращения кибератаки);
- атаки программ-вымогателей (тип кибершантажа);
- криптоджекинг (майнинг криптовалюты с использованием чужих ресурсов без ведома их владельцев);
- кибершпионаж (несанкционированное получение доступа к данным государственных или коммерческих организаций).

Возвращаясь к вопросу «кадрового голода» в области кибербезопасности субъектов финансового сектора и крупных отечественных компаний разных отраслей, отметим, что на практике списки открытых вакансий в отечественных компаниях в сфере кибербезопасности часто остаются незаполненными месяцами; руководство компаний бессистемно пытается восполнить эти лакуны в квалификации офисного персонала, проводя неадекватное обучение на рабочем месте в надежде, что высокотехнологические решения помогут снизить уровень киберугрозы, однако это далеко не всегда обеспечивает кибербезопасность и информационную безопасность компании в целом.

Если подготовка востребованных специалистов в области кибербезопасности будет происходить во всем мире такими же темпами, как сегодня, уровень опасности будет только расти.

Как сообщает The New York Times, аналитики известной компании по киберзащите Cybersecurity Ventures прогнозирует более 3,5 млн незаполненных рабочих мест в сфере кибербезопасности во всем мире к началу 2022 г., против одного миллиона таких же вакансий в 2014 г.[6].

По данным Минтруда РФ, к концу 2020 г. в РФ не хватало порядка 18,5 тыс. специалистов по информационной безопасности, что на 5 % меньше, чем в 2019 г. И ситуация может быть еще хуже, если система высшего образования не отреагирует своевременно на запросы работодателей. Даже если сейчас российские организации высшего образования создадут систему подготовки специалистов по кибербезопасности, потребуются годы, чтобы подготовить специалистов[7].

В настоящее время, по данным Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, в стране в контексте реализации Указа Президента РФ № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»[8] в условиях необходимости обеспечения ускоренного внедрения цифровых технологий в экономике и социальной сфере, Правительство РФ разработало и внедряет Национальный проект, именуемый Национальной программой «Цифровая экономика Российской Федерации»[9], нацеленной на увеличение

[4] Cyber crime: understanding the online business model. National Cyber Security Center. 2017. URL: https://www.ncsc.gov.uk/files/Cyber%20crime%20-%20understabnding%20the%20online%20business%20model.pdf (дата обращения: 01.10.2021).

[5] «Лаборатория Касперского» – международная компания, работающая в сфере информационной безопасности и цифровой приватности с 1997 г. Глубокие экспертные знания и многолетний опыт компании лежат в основе защитных решений и сервисов нового поколения, обеспечивающих безопасность бизнеса, критически важной инфраструктуры, государственных органов и рядовых пользователей. Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для защиты конечных устройств, а также ряд специализированных решений и сервисов для борьбы со сложными и постоянно эволюционирующими киберугрозами. URL: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime (дата обращения: 21.12.2021).

[6] *Paulette Perhach.* The Mad Dash to Find a Cybersecurity Force. The New York Times. No. 7, 2018. URL: https://www.nytimes.com/2018/11/07/business/the-mad-dash-to-find-a-cybersecurity-force.html (дата обращения: 01.10.2021).

[7] Это данные Министерства труда и социальной защиты России, приведенные по итогам исследования, в котором приняли участие более 15 тыс. российских компаний. URL: https://bizgaz.ru/2021/02/26/kiberbezopasnost-ili-prichem-tut-kadrovyj-golod.html (дата обращения: 01.10.2021).

[8] О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года: Указ Президента Рос. Федерации от 7 мая 2018 г. № 204 (в ред. от 21 июля 2020 г.).

[9] Паспорт национального проекта Национальной программы «Цифровая экономика Российской Федерации» утвержден протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7.

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.

Однако указанные в Паспорте национального проекта Национальной программы «Цифровая экономика Российской Федерации» цели не отражают в полной мере проблему информационной безопасности финансового сектора российской экономики и ее кадрового обеспечения.

В структуру рассматриваемого национального проекта входит шесть федеральных проектов: «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 в статье проблемы, а также подчеркивают факт проявления внимания руководства страны к решению указанных вопросов.

Хотя Федеральный проект «Информационная безопасность» нацелен на решение вопросов, связанных с обеспечением информационной безопасности (ИБ) на основе отечественных разработок, по мнению авторов настоящей статьи, эффект от реализации Национальной программы «Цифровая экономика Российской Федерации», будет мало заметен, поскольку возникают вопросы, связанные с отсутствием единого подхода к процессу стратегирования ИБ как на региональном, муниципальном, так и на корпоративном уровне, хотя действует множество указов Президента России и федеральных законов. Прокомментируем некоторые положения из них.

В *Конституции Российской Федерации* определено, что в ведении РФ находятся оборона и безопасность, в том числе безопасность личности, общества и государства при применении информационных технологий (ИТ) и обороте цифровых данных.

В *Стратегии национальной безопасности Российской Федерации*[10] (далее – Стратегия) указано, что национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией и законодательством РФ, а именно государственную, общественную, *информационную*, экологическую, экономическую, транспортную, энергетическую безопасность и безопасность личности. Там же дано определение понятия «обеспечение национальной безопасности»[11]. В Стратегии подчеркнуто, что одним из главных направлений обеспечения национальной безопасности *в области науки, технологий и образования* является повышение уровня технологической безопасности, в том числе в информационной сфере. Стратегия также содержит ряд положений об отставании России в разработке и внедрении перспективных технологий, *незащищенности национальной финансовой системы от действий нерезидентов и спекулятивного иностранного капитала, уязвимости информационной инфраструктуры* и др., о необходимости усиления роли государства в качестве гаранта безопасности личности и прав собственности, совершенствования правового регулирования предупреждения преступности (в том числе в информационной сфере), принятия активных мер по государственной защите российских производителей, осуществляющих деятельность в области военной, продовольственной, *информационной* и энергетической *безопасности*. В последних положениях Стратегии отмечено, что при ее реализации «особое внимание уделяется обеспечению информационной безопасности с учетом стратегических национальных приоритетов».

Доктрина информационной безопасности Российской Федерации[12] (далее – Доктрина) была утверждена через год после Стратегии. В ней определены такие понятия, как «информационная безопасность Российской Федерации»[13], «угроза информационной безопасности Российской Федерации», «обеспечение информационной безопасности»; «силы обеспечения информационной безопасности», «средства обеспечения информационной безопасности», «система обеспечения информационной безопасности», «информационная инфраструктура Российской Федерации»[14]. В Доктрине определены положе-

[10] Утв. Указом Президента России от 31 декабря 2015 г. № 683.

[11] Определение понятия «обеспечение национальной безопасности» трактуется в Стратегии как «реализация органами государственной власти и органами местного самоуправления во взаимодействии с институтами гражданского общества политических, военных, организационных, социально-экономических, информационных, правовых и иных мер, направленных на противодействие угрозам национальной безопасности и удовлетворение национальных интересов».

[12] Утв. Указом Президента России от 5 декабря 2016 г. № 646.

[13] Информационная безопасность РФ определена в Доктрине информационной безопасности как «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие РФ, оборона и безопасность государства».

[14] Информационная инфраструктура РФ в Доктрине определена как «совокупность объектов информатизации, информационных систем, сайтов в сети Интернет и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации».

ния о национальных интересах в информационной сфере и их защите, в том числе в области: а) развития в РФ отрасли ИТ и электронной промышленности, а также совершенствования деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения ИБ, оказанию услуг в области обеспечения ИБ; б) содействия формированию системы международной ИБ, направленной на противодействие угрозам использования ИТ в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области ИБ, а также на защиту суверенитета РФ в информационном пространстве; г) реализации национальных интересов в информационной сфере, направленной на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности РФ. В Доктрине отмечено, что «практика внедрения ИТ без увязки с обеспечением ИБ существенно повышает вероятность проявления *информационных угроз*», а одним из основных негативных факторов, влияющих на повышение уровня информационных угроз и состояние ИБ в целом, «является наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях».

В Доктрине определены стратегические цели и основные направления обеспечения ИБ, в том числе:

– основные направления обеспечения ИБ в области государственной и общественной безопасности;

– стратегические цели обеспечения ИБ в экономической сфере, направленные на «сведение к минимально возможному уровню влияния негативных факторов, обусловленных недостаточным уровнем развития отечественной отрасли ИТ и электронной промышленности, разработку и производство конкурентоспособных средств обеспечения ИБ, а также повышение объемов и качества оказания услуг в области обеспечения ИБ»;

– основные направления обеспечения ИБ в экономической сфере, среди которых следует выделить «инновационное развитие отрасли ИТ и электронной промышленности, увеличение доли продукции этой отрасли в ВВП, в структуре экспорта страны»; «повышение конкурентоспособности российских компаний, осуществляющих деятельность в отрасли ИТ и электронной промышленности, разработку, производство и эксплуатацию средств обеспечения ИБ, оказывающих услуги в области обеспечения ИБ, в том числе за счет создания благоприятных условий для осуществления деятельности на территории РФ».

В Доктрине в качестве стратегической цели обеспечения ИБ *в области науки, технологий и образования* заявлена «поддержка инновационного и ускоренного развития системы обеспечения ИБ, отрасли ИТ и электронной промышленности», а среди ее основных направлений – «достижение конкурентоспособности российских ИТ и развитие научно-технического потенциала в области обеспечения ИБ»; «проведение научных исследований и осуществление опытных разработок в целях создания перспективных ИТ и средств обеспечения ИБ»; «*развитие кадрового потенциала в области обеспечения ИБ и применения ИТ*»; «обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной ИБ».

В последнем разделе Доктрины, посвященной организационным основам обеспечения ИБ, раскрываются положения о создании и функционировании системы обеспечения ИБ как части системы обеспечения национальной безопасности РФ и формулируются задачи государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения ИБ.

В Федеральном законе «О безопасности критической информационной инфраструктуры Российской Федерации»[15], принятым через год после утверждения Доктрины, даны определения таким понятиям, как «критическая информационная инфраструктура[16]» (КИИ), «объекты критической информационной инфраструктуры», «субъекты критической информационной инфраструктуры[17]», «безопасность критической информационной инфраструктуры[18]», «значимый объект критической информационной

[15] Утв. 26 июля 2017 г. № 187-ФЗ.

[16] Согласно Закону, КИИ объединяет объекты КИИ (информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов).

[17] Субъектами ГИИ названы в Законе государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели (ИП), которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, *банковской сфере и иных сферах финансового рынка*, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) ИП, которые обеспечивают взаимодействие указанных систем или сетей.

[18] Безопасность КИИ в Законе трактуется как состояние защищенности КИИ, обеспечивающее ее устойчивое *функционирование при проведении в отношении ее компьютерных атак*, а компьютерная атака – как целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты КИИ, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

инфраструктуры», «компьютерная атака», «компьютерный инцидент»[19]; раскрыты основы правового регулирования отношений в области обеспечения безопасности КИИ, сформулированы принципы обеспечения безопасности КИИ (законность; непрерывность и комплексность обеспечения безопасности КИИ, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов КИИ; приоритет предотвращения компьютерных атак), определены положения, характеризующие функционирование государственной система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, распределение полномочий Президента России и органов государственной власти РФ в области обеспечения безопасности КИИ; классифицированы категории объектов КИИ; определены права и обязанности субъектов КИИ, условия создания и функционирования системы безопасности значимого объекта КИИ, требования по обеспечению безопасности значимых объектов КИИ, механизмы оценки безопасности КИИ и государственного контроля в области обеспечения безопасности значимых объектов КИИ, а также порядок ведения реестра значимых объектов КИИ.

Возвращаясь к анализу содержания Национальной программы «Цифровая экономика Российской Федерации» отметим, что особое значение в контексте темы настоящего исследования, имеет упомянутый выше Федеральный проект «Кадры для цифровой экономики», нацеленный на «обеспечение подготовки высококвалифицированных кадров для цифровой экономики». Как показывает анализ Паспорта национального проекта рассматриваемой Национальной программы, вопрос о кадровом обеспечении информационной безопасности финансового сектора российской экономики остается открытым. В Паспорте заявлено 32 позиции, деликатно обходящие данный вопрос, имеющий, очевидно, для информационной безопасности финансового рынка РФ первостепенное значение.

В 2018 г. был введен в действие весьма важный документ «ГОСТ Р 57580.1–2017. Национальный стандарт РФ. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»[20], знание и руководство которым, по мнению авторов настоящей статьи, необходимо практически любому работнику субъекта финансового сектора, как и знание еще более важного стандарта по рассматриваемой тематике настоящего исследования «ГОСТ Р ИСО/ТО 13569–2007. Национальный стандарт РФ. Финансовые услуги. Рекомендации по информационной безопасности»[21], содержащего разделы «Политика информационной безопасности организации», «Менеджмент информационной безопасности. Программа обеспечения безопасности», «Структура информационной безопасности», «Анализ и оценка риска», «Выбор и внедрение защитных мер» (по обеспечению ИБ), «Меры защиты систем информационных технологий», «Внедрение специальных средств защиты», «Разрешение инцидентов» и др. Оба стандарта имеют ценные практико-ориентированные приложения.

В России действуют и профессиональные стандарты, являющиеся своего рода выражением спроса работодателей на рабочую силу, они были приняты несколько раньше (в 2015–2016 гг.), поэтому вопрос о компетентности работников субъектов финансового сектора в области информационной, цифровой безопасности там не нашел должного отражения.

Так, например, в профессиональных стандартах специалиста по платежным системам[22], специалиста по платежным услугам[23], специалиста по дистанционному банковскому обслуживанию[24] существенные аспекты обеспечения информационной безопасности в трудовых функциях указанных специалистов не получили отражения.

Отечественное бизнес-сообщество крайне обеспокоено данными вопросами: Совет ТПП РФ по финансово-промышленной и инвестиционной политике в июне 2020 г. провел вебинар для представителей предпринимательского сообщества и торгово-промышленных палат по теме «Информационная безопасность для финансовых организаций»[25]. Подобные вебинары часто инициируют ведущие экономические вузы страны (РАНХиГС при Президенте России, Финансовый университет при Правительстве РФ, Российский экономический университет имени Г.В. Плеханова и др.).

[19] В Законе введено также понятие компьютерный инцидент, который определен как факт нарушения и (или) прекращения функционирования объекта КТТ, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

[20] Утв. Приказом Росстандарта от 8 августа 2017 г. № 822-ст. Дата введения ГОСТа – 1 января 2018 г.

[21] Утв. Приказом Ростехрегулирования от 27 декабря 2007 г. № 514-ст. Дата введения ГОСТа – 1 июля 2008 г.

[22] Стандарт зарегистрирован Приказом Минюста России от 31 марта 2015 г. № 204н.

[23] Стандарт зарегистрирован Приказом Минюста России от 14 ноября 2016 г. № 645н.

[24] Стандарт зарегистрирован Приказом Минюста России от 19 апреля 2017 г. № 366н.

[25] Вебинар «Информационная безопасность организации. Что необходимо знать руководителю?» РАНХиГС, 18 марта 2021 г. URL: https://www.ranepa.ru/sobytiya/aktsii-meropriyatiya/vebinar-informatsionnaya-bezopasnost-organizatsii-chto-neobkhodimo-znat-rukovoditelyu-/ (дата обращения: 01.10.2021).

Вопрос об обеспечении информационной безопасности стоит весьма остро не только внутри страны, но и на международном уровне. Так, 25 сентября 2020 г. президент РФ В.В. Путин выступил с заявлением о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности[26].

Ключевой проблемой обеспечения информационной безопасности финансового сектора, тормозящей полноценный, быстрый и безболезненный переход к цифровой экономике, является несоответствие спроса финансовых организаций на кадры предложениям отечественного рынка труда. Важно отметить, что в Атласе новых профессий 3.0, разработанных Сколково и Агентством стратегических инициатив, указана профессия «Аналитик кибербезопасности в финансовом секторе» [12], 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 [13].

Вероятно, наряду с профессией аналитика кибербезопасности, в финансовом секторе понадобятся разработчики, производители и администраторы систем информационной безопасности, а также промоутеры цифровой финансовой грамотности населения. Отсутствие специалистов в перечисленных сферах цифровой экономики потребует соответствующих изменений в действующем законодательстве, в порядке работы органов государственной власти, органов местного самоуправления, деятельности производственных компаний, финансовых и некоммерческих организаций; понадобятся юристы и государственные (муниципальные) служащие, специализирующиеся по актуальным вопросам обеспечения информационной безопасности и защиты от киберугроз. Очевидно, что должны быть созданы новые федеральные государственные образовательные стандарты (ФГОС) среднего профессионального образования и высшего образования (бакалавриат, специалитет, магистратура). Существующие ФГОС, нацеленные на подготовку специалистов в области современных информационных технологий и обеспечения информационной безопасности, ориентированы исключительно на подготовку технических специалистов, что указывает на системный и организационный разрыв между потребностями рынка труда и возможностями системы профессионального образования.

Как отмечают иностранные исследователи, проблему информационной безопасности финансового сектора требуется решать комплексно [14–15], так как стратегическое, тактическое и операционное управление системой кадрового обеспечения информационной безопасности финансового сектора представляется весьма важным и приоритетным не только для субъектов финансового сектора, но и общества в целом.

Организационно-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, решению глобальных проблем современности и 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 архитекторы информационной среды, создатели контента, разработчики и администраторы средств массовой коммуникации, высокотехнологического оборудования и наукоемких технологий.

С ростом числа хакерских групп, мощных по воздействию используемых ими моделей и инструментов, подпольных форумов, а также финансовых и деструктивных мотивов, повышающих уровни киберугроз, бизнес-сообщество должно быть способно отразить кибератаку или применить эффективные средства киберзащиты, что предопределяет необходимость:

1) развития навыков: компании (финансовые организации и другие субъекты экономики) должны инвестировать в рост и развитие навыков, идущих в ногу с новыми технологиями, так как повышение ИТ-квалификации персонала является критически важным приоритетом во всех областях цифровой экономики, включая деятельность субъектов финансового сектора, образовательных учреждений профессионального образования, субъектов сектора государственного (муниципального) управления и др.;

2) многосторонняя поддержка и новые технологии: компании должны привлекать сторонние организации, которые специализируются на кибербезопасности и круглосуточно «пристально следят за грозовым киберoблаком», в сочетании с технологиями искусственного интеллекта (AI) и машинного обу-

[26] Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности. URL: http://kremlin.ru/events/president/news/64086 (дата обращения: 01.10.2021).

чения (ML), чтобы выявлять и смягчать появление и распространение киберугрозы «Zero Дня».

Компании (финансовые организации) должны проявлять изобретательность и отражать эти контратаки новаторскими и продуманными способами. Подходы, которые на сегодняшний день доказали свою эффективность, включают:

– выращивание и поощрение талантливых специалистов внутри компании;

– активное участие в программах повышения квалификации и переподготовки персонала в рассматриваемой области;

– инвестирование во внешние аутсорсинговые службы безопасности для защиты уязвимых брешей и улучшения общего состояния в области кибербезопасности.

Министр цифрового развития Максут Шадаев считает, что в цифровой отрасли «необходимо стимулировать спрос – и здесь локомотивом будут госкомпании, госкорпорации». Острым вопросом в цифровой экономике, по его мнению, является дефицит кадров на ИТ-рынке. К 2024 г. планируется двукратное увеличение бюджетных мест на ИТ-специальности в российских вузах. С 2021 г. введена адаптация образовательных программ ведущих университетов к современным реалиям и запущена массовая переподготовка преподавателей в сфере кибербезопасности[27].

Литература

1. *Dufva T., Dufva M.* Grasping the future of the digital society // Futures. 2019. Vol. 107. PP. 17–28.

2. *van Dijck J.* Governing digital societies: Private platforms, public values // Computer Law & Security Review. 2020. Vol. 36: 105377. PP. 3–4.

3. *Nicholas Negroponte.* Being digital / First published in Great Britain in 1995 by Hodder and Stoughton. London: Published by arrangement with Alfred A. Knopf, Inc. 1995. 252 p. URL: https://governance40.com/wp-content/uploads/2018/12/Nicholas-Negroponte-Being-Digital-Vintage-1996.pdf.

4. *Tapscott D., Williams A.D.* Radical Openness: Four Unexpected Principles for Success. (Kindle Edition), TED Conferences; 28th edition (January 17, 2013). 71 p.

5. *Глазьев С.* Великая цифровая экономика // Социальная политика и социальное партнерство. 2017. № 11. С. 5–26.

6. *Глазьев С.Ю.* Об использовании цифровых технологий в целях создания рынка капитала ЕАЭС // Евразийская интеграция: экономика, право, политика. 2018. № 1 (23). С. 7–8.

7. *Китова О.В.* Актуальные вопросы развития цифрового государства в России // Научные труды Вольного экономического общества России. 2021. Т. 230, № 4. С. 211–216.

8. *Марамыгин М.С., Чернова Г.В., Решетникова Л.Г.* Цифровая трансформация российского рынка финансовых услуг: тенденции и особенности // Управленец. 2019. Т. 10, № 3. С. 70–82.

9. *Пороховский А.А.* Цифровизация и искусственный интеллект: перспективы и вызовы // Экономика. Налоги. Право. 2020. Т. 13, № 2. С. 84–91.

10. *Новиков А.И.* Вопросы методологии и гносеологии в развитии цифровой экономики // Теоретическая экономика. 2019. № 10 (58). С. 26–31.

11. *Янгиров А.В., Мухаметова А.Д.* Особенности управления региональным развитием в условиях цифровизации // Экономика и управление: научно-практический журнал. 2020. № 5 (155). С. 31–33.

12. Атлас новых профессий 3.0 / Под ред. Д. Варламовой, Д. Судакова. М.: Альпина. М.: Интеллектуальная Литература, 2020. 456 с. URL: https://storage.tusur.ru/files/133096/Atla s_3.0.pdf.

13. *Macnish K., Ham J.* Ethics in cybersecurity research and practice // Technology in Society. 2020. Vol. 63: 101382. URL: https://www.researchgate.net/publication/346786967_Ethics_in_cybersecurity_research_and_practice (дата обращения: 21.12.2021).

14. *Chong H.-Y., Diamantopoulos A.* Integrating advanced technologies to uphold security of payment: Data flow diagram // Automation in Construction. 2020. Vol. 114: 103158. URL: https://www.sciencedirect.com/science/article/abs/pii/S0926580519313573 (дата обращения: 21.12.2021).

15. *Ficco M., Palmieri F.* Leaf: An open-source cybersecurity training platform for realistic edge-IoT scenarios // Journal of Systems Architecture. 2019. Vol. 97, PP. 107–129.

[27] В России предложили построить открытую базу знаний для антивирусных компаний. URL: https://www.cnews.ru/news/top/2021-09-28_positive_technologies_predlozhila_novyj.