РОССИЙСКИЙ БИЗНЕС НА ПОВОРОТНОМ ЭТАПЕ

ПЕРСПЕКТИВЫ ЭКСПОРТА РОССИЙСКИХ ПРОДУКТОВ И УСЛУГ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. НОВЫЕ РЫНКИ И ВОЗМОЖНОСТИ В УСЛОВИЯХ САНКЦИОННОГО ДАВЛЕНИЯ (НА ПРИМЕРЕ ОЦЕНКИ РЫНКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СТРАНАХ БЛИЖНЕГО ВОСТОКА И СЕВЕРНОЙ АФРИКИ)

Хусаинова А.И.[18], Мытенков С.С.[19]

Данная статья посвящена оценке состояния рынка информационной безопасности в Российской Федерации применительно к финансовому сектору российской экономики, а также оценке экспортного потенциала отечественных продуктов и услуг в области кибербезопасности в странах Ближнего Востока и Северной Африки.

Значимость и прикладная ценность исследования состоит в актуальности рассматриваемой авторами проблемы. В условиях жесткого санкционного давления и возрастающей конкуренции на внутреннем рынке перед менеджментом российских компаний, разрабатывающих продукты и, предоставляющих услуги в сфере обеспечения информационной безопасности, предстает задача определить наиболее перспективные с точки зрения диверсификации зарубежные рынки сбыта. Особое внимание авторы статьи уделяют оценке текущего состояния рынков кибербезопасности и развитию финансового сектора в регионе Ближнего Востока и Северной Африки.

Ключевые слова:

кибербезопасность, информационная безопасность, финансовый сектор, экспортный потенциал, Ближний Восток, Северная Африка.

[18] **Хусаинова Анастасия Ильясовна** - слушатель общеуниверситетского факультатива «GR в современной России: теория и практика» кафедры теории и практики взаимодействия бизнеса и власти НИУ «Высшая школа экономики». Электронная почта: anastasia.khusainova.26@yandex.ru.

[19] **Мытенков Сергей Сергеевич** - старший преподаватель кафедры теории и практики взаимодействия бизнеса и власти НИУ «Высшая школа экономики». Вице-президент - Управляющий директор Управления регионального развития Российского союза промышленников и предпринимателей. Рабочий телефон: +7 (495) 663 04 04 (доб. 1150).

Введение

Информационная безопасность (далее – ИБ) или кибербезопасность в 21 в. является одной из ключевых областей, которой компании и государства по всему миру уделяют значительное внимание. Значение кибербезопасности сложно переоценить. Ввнедрение современных решений позволяет не только отражать бесконечное число кибератак, нацеленных на совершение преступлений с целью получения финансовой выгоды, но и обеспечивает стабильность функционирования значимых объектов военной, социальной, топливно-энергетической, атомной и многих других, значимых для государства, отраслей.

Первая кибератака на объект критической инфраструктуры произошла задолго до появления Интернета в 1982 г., когда посредством установки трояна в SCADA-систему был осуществлен подрыв сибирского нефтепровода [3]. Самой крупной кибератакой в финансовом секторе стал вирус Carbanak, затронувший порядка 100 финансовых учреждений по всему миру. Первой жертвой Carbanak стал украинский банк, после чего хакеры осуществили атаку на российский банк, уведя с корреспондентского счета ПИР Банка 58 млн руб. Затем атакам подверглись банки по всему миру. Больше всего от вируса пострадали банки в России, США, Германии, Китае и Украине. Вирус затронул финансовые организации на всех континентах, нанеся ущерб, оценивающийся в сумму порядка 1 млрд. долл. [9]. Согласно исследованию компании Positive Technologies, общее количество кибератак, приведших к негативным последствиям для юридических и физических лиц, в России по итогам 2022 г. возросло на 20,8%. Увеличилось количество массовых утечек информации, приводящее к атакам с использованием скомпрометированной информации (см. рис. 1). Количество атак на блокчейн-платформы и веб-ресурсы в 2022 г. возросло более чем в 2 раза [1]. Кратный рост числа киберпреступлений объясняется ростом напряженности на геополитической арене, ставшей результатом начала специальной военной операции в Украине. Больше всего от кибератак пострадали веб-ресурсы государственных учреждений, СМИ и транспортного сектора (см. рис. 2).

Рис. 1. Типы украденных данных в успешных атаках, совершенных в отношении физических лиц и организаций в 2022 г. в России

Рис. 2. Доля инцидентов, связанных с атаками на веб-ресурсы в разбивке по секторам российской экономики в 2021-2022 гг.

Финансовый сектор традиционно считается наиболее подверженным кибератакам. Несмотря на усилия, прикладываемые государством и финансовыми учреждениями для повышения уровня ИБ, количество киберпреступлений ежегодно возрастает. Согласно отчету компании StormWall, финансовый сектор российской экономики занимал лидирующую позицию по количеству DDoS-атак по итогам первого полугодия 2022 г., увеличившихся в 12,8 раз по сравнению с аналогичным периодом прошлого года (см. рис. 3). Ключевой целью таких атак является доведение систем и сетевых служб до отказа, когда ресурс становится недоступным для добросовестных пользователей в результате захвата всех свободных ресурсов злоумышленниками, осуществляющими массовое подключение с разных устройств.

Рис. 3. Количество DDoS-атак в России по секторам в I полугодии 2022 г.

В результате введения санкций со стороны западных государств, подавляющее число российских компаний из ключевых секторов экономики столкнулось с беспрецедентной проблемой замещения ушедших с рынка продуктов и услуг. Стоит отметить, что рынок ИТ-продуктов оказался под бóльшим ударом по сравнению с рынком ИБ. Несмотря на практически повсеместное использование иностранных продуктов и услуг в части обеспечения ИБ, компании постепенно переходят на отечественные аналоги. Возрастающая на рынке конкуренция приводит к тому, что российские вендоры стремятся к усовершенствованию своих решений с целью как можно быстрее занять освободившиеся ниши. Качество продуктов по-прежнему отстает от развитых зарубежных технологий, однако несмотря на это отечественные вендоры еще до начала военного конфликта в Украине начали освоение зарубежных рынков сбыта, составляя конкуренцию таким гигантам как Cisco и IBM. Успешный опыт Лаборатории Касперского и Softline

вкупе с улучшением условий ведения бизнеса для иностранных компаний в некоторых странах ближневосточного региона могут стать хорошим подспорьем для развития российских компаний за рубежом.

Рынок информационной безопасности в России

По различным оценкам в денежном выражении рынок ИБ в России по итогам 2021 г. оценивался в диапазоне от 185,9 [19] до 220,3 [16]. Согласно исследованию аналитиков компании «Ростелеком-Солар», объем рынка в денежных тратах конечных пользователей за 2021 г. оценивается на уровне 98,6 млрд руб. [13]. Около 61% вендоров в сфере кибербезопасности в России еще в 2021 г. представляли отечественные компании, в то время как доля зарубежных вендоров составляла 39% - более 1/3 рынка. В 2022 г. ситуация начала кардинально меняться на фоне введения санкций и неопределенности, возникшей в результате негативных геополитических событий. Указом Президента от 30.03.2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» с 31.03.2022 г. введен запрет на закупку иностранного программного обеспечения (далее – ПО) и программно-аппаратных комплексов (далее – ПАК) для использования на объектах критической информационной инфраструктуры (далее – КИИ), а с 01.01.2025 г. в силу вступает запрет на использование иностранного ПО и ПАК для использования на объектах КИИ[20]. Введение вышеупомянутых запретов подвигло подавляющее большинство иностранных компаний к выводу своих активов с российского рынка. В марте 2022 г. российский рынок покинуло ок. 15 компаний, среди которых оказались такие гиганты как Microsoft, Cisco, Fortinet, IBM и др. Ввиду того, что уход с рынка невозможно осуществить одномоментно, поскольку контракты между вендорами и заказчиками заключаются на несколько лет, многие компании продолжают пользоваться иностранным ПО, параллельно активно замещая эти продукты отечественными разработками. Согласно прогнозу аналитиков Центра стратегических разработок (ЦСР), в 2023 г. доля иностранных вендоров может сократиться до рекордных 5%.

Ключевой тенденцией российского рынка ИБ в 2022-2023 гг. стал масштабный переход компаний на отечественное ПО. Иностранные компании, предоставлявшие ранее свои решения и услуги в сфере информационных технологий, в том числе в области ИБ, продолжают покидать рынок. Часть лицензий, предоставленных до 24 февраля 2022 г., продолжает действовать, однако по истечении срока действия этих лицензий, иностранные вендоры прекратят оказание технической поддержки своих программных продуктов, что приведет к невозможности эксплуатации иностранного ПО. Лишившись доступа к иностранному ПО и инфраструктуре, состоящей в основном из импортных комплектующих, а также учитывая введение запрета на закупку и использование иностранного ПО и ПАК на объектах КИИ, российские компании стали повсеместно включать проекты, направленные на импортозамещение, в собственные стратегии долгосрочного развития и цифровой трансформации. Все

[20] К критической информационной инфраструктуре (КИИ) относятся объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов. К объектам КИИ относят информационные системы (ИС), информационно-телекоммуникационные сети (ИТС), а также автоматизированные системы управления (АСУ) субъектов КИИ. К субъектам КИИ относятся государственные органы и учреждения, российские юридические лица и (или) индивидуальные предприниматели (ИП), которым на праве собственности, аренды или на ином законном основании принадлежат объекты КИИ, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных ключевых сферах российской экономики, а также российские юр. лица и (или) ИП, обеспечивающие взаимодействие этих систем или сетей.

вышеперечисленные факторы подстегивают спрос на отечественное ПО и инфраструктуру, оказывая положительное влияние на развитие отечественных компаний. Согласно прогнозу ЦСР, доля зарубежных вендоров, поставляющих продукты и услуги в области кибербезопасности, снизится с 73 млрд. руб. в 2021 г. до 23 млрд. руб. в 2026 г. (см. рис. 4) [19].

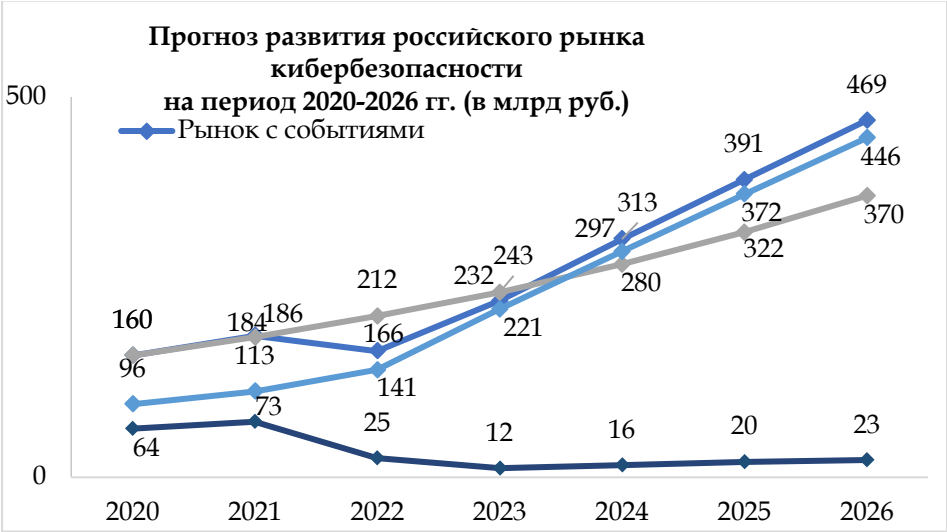

Рис.4. Прогноз развития российского рынка кибербезопасности на период 2020-2026 гг. (в млрд руб.).

В таблице 1 приводится статистика за 2020-2021 гг. по выручке крупнейших российских вендоров, предоставляющих свои продукты и услуги в сфере обеспечения ИБ. Согласно этим данным, в 2021 г. в ТОП-3 крупнейших по выручке компаний входили Лаборатория Касперского, Softline и ГК Цитадель.

Таблица 1

Выручка крупнейших компаний России, осуществляющих деятельность в сфере защиты информации, за 2020-2021 гг. [16]

	Компания	**Выручка в 2021 г., в млрд руб., с НДС**	**Выручка в 2020 г., в млрд руб., с НДС**	**Рост выручки 2021/2020, в %**
	Лаборатория Касперского	55,8	50,6	10,2%
	Softline	22,3	20,3	9,8%
3	Цитадель	19,0	20,5	-7,4%
4	Ростелеком-Солар	12,3	8,4	46,9%
	Bi.Zone	10,4	9,0	16,5%
	Инфосистемы Джет	8,8	7,0	26,8%
	ИнфоТеКС	8,5	7,3	16,1%
	Positive Technologies	7,6	6,0	27,8%
	Innostage	7,3	4,6	57,5%
0	Норси-Транс	5,8	9,5	-39,2%

1	Информзащита	5,8	6,4	-9,8%
2	Код безопасности	5,3	5,9	-8,9%
3	Angara Security	5,2	3,3	59,1%

До начала событий 2022 г. Лаборатория Касперского и Softline активно продвигала свои решения на зарубежных рынках, в том числе и в недружественных странах. В 2022 г., осуществив покупку Seven Seas Technology - ведущего системного интегратора и поставщика решений в области информационно-коммуникационных технологий в ОАЭ, Softline переориентировала свою стратегию развития на рынки стран Ближнего Востока и Африки [20]. ГК Цитадель является ключевым поставщиком систем для телекоммуникационных компаний, предназначенных для проведения оперативно-розыскных мероприятий. Доля компании на российском рынке систем оперативно-розыскных мероприятий (далее – СОРМ) составляет около 60%. Кроме того, в ГК Цитадель входят компании-разработчики решений в сфере обеспечения ИБ. ИКС Холдинг, в состав которого входит ГК Цитадель, согласно данным Коммерсанта, по итогам 2022 г. увеличил консолидированную выручку до 91 млрд. руб. (рост более чем на 115 % от года к году) [15]. Доля услуг на российском рынке кибербезопасности в 2021 г. составляла около 27%, в то время как сами средства защиты информации, в том числе ПО, составляли 73% рынка ИБ [19]. К услугам в сфере кибербезопасности относится осуществление технической поддержки и сопровождения продуктов ИБ, предоставление доступа к инфраструктурным мощностям, а также предоставление консалтинговых услуг (в т.ч. оценка уровня защищенности и проведение расследований произошедших инцидентов) [18].

Стоит отметить, что осуществление технической поддержки и сопровождения на объектах КИИ предполагает под собой более высокие требования к выполнению показателя SLA (Service Level Agreement, Соглашение об уровне качества) при отработке инцидентов. До недавнего времени не каждая аутсорсинговая компания могла обеспечить своим клиентам сервис, включающий как соблюдение специфичных отраслевых требований, так и высокие показатели SLA. Однако, в 2022 г. ситуация начала меняться. Сокращение доступной к закупке инфраструктуры, нехватка капитала и других ресурсов привели к тому, что компаниям стало выгоднее переходить на сервисную модель «Security-as-a-service» («Безопасность как сервис»). Переход российских компаний к использованию сервисной модели обеспечения ИБ стал не только последствием санкционного давления на Россию, но также является общемировым трендом, благодаря которому зарубежные компании экономят значительные средства на обеспечении ИБ.

Согласно данным, опубликованным на сайте независимого российского информационно-аналитического центра Anti-Malware, на текущий момент российский рынок ИБ имеет достаточное количество отечественных аналогов продуктов ИБ в большинстве классов средств защиты информации. Разработка аналогов зарубежных продуктов кибербезопасности началась задолго до событий февраля 2022 г. По этой причине российские вендоры были подготовлены к столь революционному по своим масштабам импортозамещению продуктов и услуг, обеспечивающих защиту информации [8]. Ввиду неожиданного роста рынка кибербезопасности в 2022 г. на 10-20%, российские вендоры начали активно конкурировать между собой,

вкладывая средства в разработку новых и совершенствование уже существующих продуктов ИБ, за счет чего у заказчиков появилась возможность экономии на расходах в части импортозамещения продуктов и услуг зарубежных вендоров [12]. Несмотря на колоссальное санкционное давление, отечественным компаниям удалось разработать аналоги даже таких относительно новых продуктов как BAS (Breach and Attack Simulation) и Threat Intelligence. BAS представляет собой технологию, которая предназначена для тестирования уязвимостей инфраструктуры посредством симуляции реальных кибератак. Threat Intelligence является элементом киберразведки, агрегирующим информацию о хакерских группировках, а также техниках и тактиках, применяемых хакерами при осуществлении кибератак. В свете многократно возрастающего числа кибератак, BAS становится одним из наиболее эффективных инструментов защиты ИБ, поскольку позволяет устранить уязвимости в системе задолго до наступления критического события.

Однако, несмотря на позитивный тренд, на текущий момент не все иностранные решения могут быть замещены качественными российскими аналогами. Сложности импортозамещения наблюдаются в такой категории продуктов как средства защиты контейнеров. Сейчас единственным российским аналогом таких средств защиты является одноименный продукт компании Luntry. Контейнеры представляют собой небольшие независимые облачные сервисы, позволяющие упростить и ускорить процесс разработки ИТ-продуктов. Технология контейнеризации стала набирать популярность в связи с активным переходом многих крупных компаний, в том числе в банковском секторе, с монолитных архитектурных решений на микросервисную архитектуру. На текущий момент на российском рынке отсутствуют аналоги таких зарубежных разработок как CASB (Cloud Access Security Broker) и SASE/SSE (Secure Access Service Edge / Security Service Edge). Это унифицированные инструменты безопасности, позволяющие обеспечить безопасность при работе с облачными решениями. Но ввиду сложности развертывания технологии, эти решения все еще не приобрели достаточной популярности на российском рынке.

Несмотря на сложности, с которыми сталкиваются российские разработчики средств защиты ИБ, по оценкам аналитиков, в ближайшей перспективе российский рынок ИБ имеет значительный потенциал к росту и уже в этом году сможет стать рынком отечественного производителя. Это, безусловно, положительный тренд для российской экономики и неплохой шанс для отечественных компаний не только занять освободившиеся ниши, но и попытаться диверсифицировать свой бизнес за счет выхода на зарубежные рынки дружественных по отношению к России стран.

Рынок информационной безопасности стран Ближнего Востока и Северной Африки

В свете геополитической напряженности на мировой арене и потери партнерских отношений с Западом все более актуальным становится вопрос налаживания отношений с дружественными по отношению к России странами. Наиболее перспективными с точки зрения экспортного потенциала видятся страны Ближнего Востока и Северной Африки. Основным источником доходов стран, входящих в этот регион, как и в России, является выручка, получаемая от продажи углеводородов, в основном от нефти. Саудовская Аравия, ОАЭ, Египет, Израиль и другие страны региона имеют хорошие экономические перспективы: низкий уровень инфляции вкупе со стремлением к развитию IT-отрасли становятся отличной почвой для привлечения инвестиций со всего мира. Еще одним значимым фактором развития рынка ИБ в этих странах, стало начало военной мобилизации на территории Российской Федерации в сентябре 2022 г.

Данное событие стало причиной отъезда большого количества высококвалифицированных специалистов из ИТ-отрасли. Многие ИТ-специалисты переехали в ближневосточные страны, продолжая работать удаленно на российские компании, либо открывая собственные ИТ-стартапы. Банковская сфера стала одной из тех ключевых отраслей, которая столкнулась с очень большой нехваткой ИТ-специалистов, поскольку текущее законодательство не позволяет сотрудникам работать, находясь за пределами страны.

Основными причинами, по которым айтишники эмигрируют в страны Ближнего Востока, являются ощутимые меры поддержки для релокантов со стороны нанимающих компаний, большие инвестиции в развитие ИТ-кластеров и смягчение требований законодательства со стороны государства. Примерами такой поддержки являются запуск IT-хаба Garage в Саудовской Аравии, название которого отсылает к истории происхождения таких гигантов, как Apple и Google [6], а также появление в 2019 г. на территории ОАЭ в эмирате Абу-Даби глобальной технологической экосистемы Hub71, которая объединила в себе огромное количество стартапов, технологических компаний, акселераторов, венчурных инвесторов, корпораций и университетов. Благодаря стимулирующим мерам, таким как стопроцентное субсидирование проживания и медицинского страхования, а также предоставление доступа к рынкам, капиталу и экспертному сообществу, Hub71 привлекает огромное количество молодых, талантливых и амбициозных специалистов [17].

По данным крупнейшей исследовательской компании MarketsandMarkets в странах Ближнего Востока прогнозируется более, чем двукратный рост рынка ИБ. Согласно статистике, приведенной в таблице 2, объем рынка должен увеличиться с 20,3 млрд. долл. в 2022 г. до 44,7 млрд. в 2027 г., а совокупный среднегодовой темп роста (CAGR) прогнозируется на уровне 17,1% [18].

Таблица 2

Оценка рынка информационной безопасности стран Ближнего Востока и Северной Африки

Страна		Объем рынка ИБ в 2022 г., млн долл.	CAGR 2022-2026, %	Объем рынка ИБ в 2026 г., млн долл.
	Израиль	1 330,00	13,48	2 210,00
	Иран	681,50	10,05	999,50
	Саудовская Аравия	403,80	11,83	631,60
	ОАЭ	381,50	11,24	584,10
	Египет	148,60	9,81	216,10

Рассматривая финансовый сектор, стоит отметить, что банковские системы и уровень сервиса, предоставляемый финансовыми учреждениями в странах ближневосточного региона и Северной Африки развивается очень неравномерно. Наиболее прогрессивной в этом отношении страной является ОАЭ, если быть еще точнее – эмират Дубай, ставший настоящим местом притяжения финтех-стартапов со всего мира. Данный факт обуславливается стремительным развитием цифровой экономики, в том числе, ставшей результатом последствий пандемии Covid-19, а также привлекательностью для финтех-компаний с точки зрения расширения деятельности в регионе Магриба и Ближнего Востока. Еще одним значимым фактором стало глобальное развитие электронной коммерции (E-commerce),

формирующей спрос на внедрение цифровых финансовых продуктов.

Однако, развитие финансового сектора Дубая началось еще в далеком 2004 г., когда в эмирате был открыт первый Дубайский международный финансовый центр (DIFC), ставший к февралю 2022 г. одним из 20-ти лучших мировых финансовых центров. На текущий момент DIFC включает в себя более тысячи компаний финансового и инновационного сектора и, сотрудничает более, чем с 3-мя тысячами компаний со всего мира. Ключевым фактором успеха этого центра является создание благоприятных условий для привлечения стартапов [10]. В июне 2022 г. DIFC создал венчурный фонд с общим капиталом в 100 млн. долл.. При этом сообщается, что DIFC планирует инвестировать в этот фонд 15% собственного капитала. Основной целью фонда является поддержка выхода небольших и средних стартапов на глобальные рынки, а также диверсификация развития экономики страны. Инвестиционный фонд DIFC планирует создание более 8 тыс. рабочих мест для молодых специалистов [4]. Анализируя предшествующий пандемии Covid-19 период, необходимо отметить взрывной рост финтех индустрии в период с 2012 по 2015 г. Согласно данным консалтинговой компании KPMG, инвестиции в финтех за этот период показали 10-кратное увеличение. Ключевым фактором бурного роста финтех индустрии в странах Ближнего Востока является приход международных финтех-компаний и создание благоприятного инвестиционного климата в этих странах. Для упрощения процедур ознакомления с местным законодательством и привлечения международных игроков, в ОАЭ создаются специальные экономические зоны, в которых существуют независимые юрисдикции и функционирует упрощенное законодательство. На рис. 5 приводится перечень ключевых преимуществ, благодаря которым финансовый сектор эмирата Дубай привлекает инвестиции со всего мира.

Рис. 5. Ключевые преимущества инвестирования в финансовый сектор Дубая.

Говоря об остальных странах Ближнего Востока и Северной Африки, необходимо отметить, что далеко не во всех из них финансовый и цифровой сектор экономики развит столь же хорошо, как в ОАЭ. Страны Персидского залива, к которым относятся ОАЭ, Саудовская Аравия и Катар отличаются богатой развитой экономикой и, согласно данным Мирового рейтинга цифровой

конкурентоспособности, опубликованного Международным институтом развития менеджмента (IMD World Digital Competitiveness Ranking) [25] продолжают активное развитие этой сферы. Так, например, в 2020 г. ОАЭ занимали 10 место в рейтинге, уступая при этом таким странам как США, специальному административному району КНР – Гонконгу, Швеции, Дании и Сингапуру. Катар занимал 29 место, а Саудовская Аравия находилась на 36 позиции. Данные консалтинговой компании Deloitte указывают на то, что эти страны в настоящий момент отличаются высоким уровнем развития онлайн-банкинга. Стремительное развитие финтеха и цифровой экономики в этих странах свидетельствует о том, что спрос на продукты и услуги для обеспечения ИБ в этих сферах будет ежегодно возрастать.

Безусловным лидером по количеству инвестиций в кибербезопасность среди стран Ближнего Востока и Северной Африки стал Израиль. Согласно данным ЦСР, по итогам 2022 г. рынок ИБ Израиля оценивался в 1,3 млрд. долл. Объем инвестиций в развитие стартапов в области ИБ в Израиле значительно превышает объемы рынка киберпреступности в этой стране. Согласно данным немецкой статистической компании Statista, в 2020 г. рынок киберпреступлений в Израиле оценивался на уровне 1 млрд. долл. [26]. Отличительной чертой израильского рынка ИБ является то, что основная часть венчурных инвестиций поступают сюда из-за рубежа, в первую очередь, от американских корпораций. Кроме того, страна может похвастаться большими объемами экспорта своих ИТ-технологий. По итогам 2021 г. Израильский институт экспорта оценивал объемы экспорта продуктов кибербезопасности на уровне 11 млрд. долл. [27]. Благодаря комплексному подходу к решению проблем в области обеспечения ИБ, в условиях непрекращающегося военного конфликта, Израилю удается не только избегать значимого ущерба инфраструктуре, но и развивать все остальные отрасли, обеспечивающие экономическое и социальное развитие в стране. Ключевым фактором успеха Израиля в развитии кибербезопасности является то, что страна стратегически подошла к решению вопроса обеспечения кадрового потенциала в сфере высоких технологий, в том числе, в области обеспечения ИБ. В некоторых израильских детских садах малыши имеют возможность с самых ранних лет знакомиться с робототехникой и освоить компьютерные навыки. В начальной школе детей обучают программированию, а в старших классах делают упор на освоение методов шифрования и борьбы с киберпреступностью. Еще одним местом, формирующим кадровый резерв из высококвалифицированных специалистов, является армия. Для того, чтобы получить отсрочку от армии, молодым парням и девушкам необходимо поступить в университет для получения технической специальности, после чего они призываются на обязательную военную службу, где продолжают развиваться в области своей специализации. Срок службы в армии составляет от 3 до 5 лет. Таким образом, к окончанию службы, молодые люди имеют хорошее образование и значительный опыт, благодаря чему могут с легкостью найти высокооплачиваемую работу в стране и за ее пределами [14]. Обладая мощными технологическими и человеческими ресурсами, Израиль стремится к международному сотрудничеству и наращивает экспортный потенциал. Согласно последним данным, самым быстрорастущим сектором экономики Израиля с точки зрения привлечения инвестиций является кибербезопасность. Далее следуют ИТ-сектор, финтех, медицинские технологии и технологии в ритейле. Израиль является привлекательным местом для международных корпораций таких как Intel, Apple и Google, что в свою очередь позволяет привлечь в страну большой поток зарубежных инвестиций и

упростить экспорт технологий за рубеж [21].

В отличие от Ближневосточного региона, страны Магриба, к которым относятся Алжир, Тунис, Марокко, Ливия и Мавритания, имеют слабо развитую экономику, что не позволяет этим странам полноценно вкладываться в развитие цифровой экономики и инвестировать средства в развитие в финтеха так же активно, как это делают богатые ближневосточные соседи. По этой причине на текущий момент развитие цифровых сервисов здесь остается в зачаточном уровне. Наиболее отсталой в этом смысле является Ливия. Сюда же можно отнести и такие ближневосточные страны, как Ирак, Иран и Палестина. В настоящий момент в Иране делают акцент на развитие технологий в военном секторе. Попытки создания в Ливане и Ираке в 2007-2010 гг. стратегии электронного правительства были преданы забвению. Стремление правительства Бахрейна к внедрению сервиса, аналогичному российским Госуслугам, привело к созданию не очень функционального сайта, который еще поддерживается в рабочем состояние, но до сих пор не пользуется большой популярностью среди населения [7]. Учитывая все вышеперечисленное, можно сделать выводы о том, что развитие рынка ИБ в этих странах в ближайшей перспективе видится крайне маловероятным.

Одним из положительных примеров развития цифрового финансового сектора среди стран Северной Африки является Алжир. До недавнего времени банковский и финансовый сектор Алжира характеризовался устаревшей технологической инфраструктурой, слаборазвитыми платежными системами и отсутствием инновационных цифровых банковских услуг. В 2021 г. Алжир начал делать первые шаги на пути к цифровизации финансового сектора, впервые запустив электронную систему онлайн платежей для почтовых и банковских платформ, позволившую связать почтовые отделения с банками. Данной услугой смогут воспользоваться около 10 млн. граждан, имеющих банковские карты [5]. Еще одним значимым примером является алжирский финтех-стартап Beyn, подписавший в качестве клиентов 11 из 19 банков, функционирующих в Алжире, которым данный стартап предоставляет цифровые банковские и платежные услуги. К успешным примерам стартапов в алжирском ИТ-секторе можно отнести разработчика ПО – Leadersoft и поставщика решений для телекоммуникационного и платежного сектора Teletic [23]. Алжир стал первой страной среди стран Магриба, создавшей Министерство по делам стартапов, которое в 2020 г. возглавил 27-летний Ясин Уалид, бывший предприниматель, признанный одним из самых влиятельных молодых африканцев рейтинга Forbes «30 до 30». Возглавив министерство, Ясин начал разрабатывать нормативно-правовую базу, способствующую развитию стартапов и, позволяющую молодым предпринимателям получать налоговые преференции для развития собственного бизнеса. По словам министра, в стране в настоящий момент ведется активная работа над реформированием законодательства для привлечения инвестиций из-за рубежа и наращивания объемов экспорта [2].

Несмотря на положительную динамику развития финтех-индустрии в Алжире, при оценке экспортного потенциала российских продуктов и услуг в области обеспечения ИБ, стоит учесть, что, несмотря на обретение независимости от Франции в 1962 г., Алжир по-прежнему остается зависим от своего колониального прошлого. Так, например, если в Тунисе и Марокко межбанковские корреспондентские отношения управляются из стран Ближнего Востока, в случае с Алжиром такое управление осуществляется из Франции. Алжирское законодательство ориентировано на опыт Франции и, поэтому вскоре после внесения изменений во французское законодательство, эти же изменения

находят свое отражение и в алжирском [24]. Говоря об алжирском рынке кибербезопасности, в том числе, в контексте развития финансового сектора, следует отметить, что экспорт российских технологий в этой стране может оказаться невостребованным, поскольку Алжир стремится к партнерству с Францией. Несмотря на содействие цифровому развитию финансового сектора со стороны государства, Алжир в значительной степени отстает от Египта и других африканских стран (см. рис. 6).

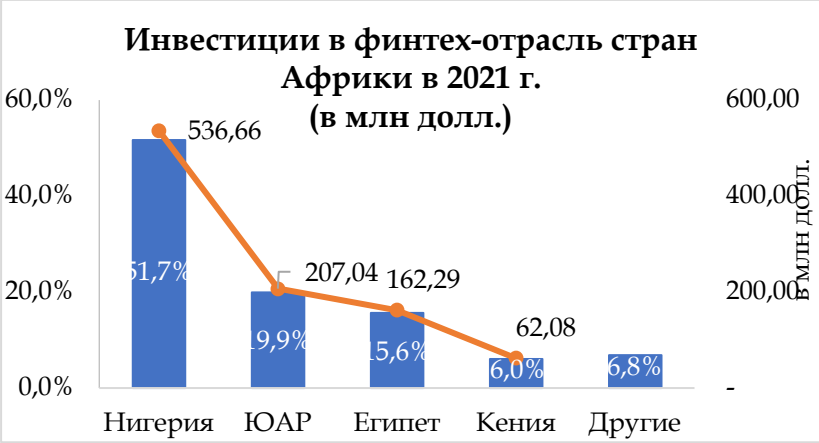

Рис. 6. Инвестиции в финтех-отрасль стран Африки в 2021 г., в млн долл.

Египет начал активно развивать финтех-индустрию еще в 2014 г. Согласно данным отчета Центрального Банка Египта за 2021 г., страна входила в ТОП-4 наиболее активных африканских стран по количеству развития финтех-стартапов на африканском континенте. Это может быть связано с интенсивным ростом финтех-индустрии за последние 7 лет: всего с 2 стартапов, появившихся в 2014 г., египетский рынок вырос до 112 финтех-компаний и стартапов к 2021 г. Ключевой проблемой развития стартапов в Египте является привлечение высококвалифицированных молодых специалистов, которые из-за большого разрыва в уровне заработных плат, высоких рисках потери работы при трудоустройстве, а также отсутствии стабильности и неизвестности будущего, предпочитают стартапам трудоустройство в крупные международные компании. По данным на 2021 г., наиболее востребованными функциями в финтех-индустрии Египта были специалисты из ИТ-сферы: потребность в их функциях составляла 57% от общего количества наиболее востребованных категорий специалистов. При этом, процент востребованности специалистов в области кибербезопасности составляла всего 12% (см. рис. 7) [22].

Рис. 7. Наиболее востребованные функции в финтех-индустрии Египта в 2021 г.

Правительство Египта создало надлежащие условия для привлечения инвестиций в развитие рынка кибербезопасности, страна привлекла огромное количество иностранных компаний, в том числе, таких гигантов как Cisco и IBM. Так, например, американский производитель средств ИБ - Sophos

планирует свое расширение на египетском рынке ИБ, который компания оценивает, как рынок с высоким потенциалом. Развитие рынка кибербезопасности Египта привлекло внимание и со стороны правительства России. В 2021 г. при содействии Минцифры РФ была организована рабочая поездка в Арабскую Республику Египет, в ходе которой российские компании высокотехнологичного сектора, в том числе, представители российского рынка кибербезопасности презентовали свои решения иностранным коллегам. Делегацию возглавил замглавы Минцифры М. Паршин. По итогам деловой поездки российская сторона увидела высокий потенциал в развитии сотрудничества с Арабской Республикой Египет в области кибербезопасности, а также в части организации экспорта и локализации российского телеком-оборудования. С египетской стороны в деловых встречах принимали участие представители Министерства связи и информационных технологий, представители Агентства по развитию информационных технологий, а также бизнес-сообщество в лице представителей компаний Telecom Egypt и ACUD. Египетские партнеры проявили высокую степень заинтересованности в развитии российско-египетских отношений [11].

Таким образом, можно сделать вывод о том, что среди стран Магриба в настоящий момент нет потенциальных партнеров, готовых к сотрудничеству с Россией в сфере развития финтех-индустрии и обеспечения ИБ. Как следствие продукты и услуги ИБ здесь в ближайшей перспективе будут не слишком востребованы. Среди стран Северной Африки наиболее перспективным видится египетский рынок ИБ.

Заключение

Анализируя российский рынок ИБ, следует отметить, что на текущий момент в стране достаточно отечественных решений, способных в обозримый промежуток времени заместить продукты и услуги зарубежных вендоров. С уходом иностранных компаний для отечественных вендоров освободилось большое количество ниш, которые в настоящий момент замещаются российскими продуктами и услугами. Возрастающая на рынке конкуренция вынуждает российские компании развивать собственные продукты, повышая уровень обеспечения ИБ во всех ключевых отраслях российской экономики. Кратное увеличение числа DDoS-атак на финансовый сектор и СМИ привело к усовершенствованию средств защиты информации. Запрет на закупку и постепенное прекращение использования иностранного ПО и ПАК на объектах КИИ привело к беспрецедентному ускорению тренда на импортозамещение. В этих условиях отечественным вендорам удалось в кратчайшие сроки закрыть потребности большинства российских компаний. Наиболее логичным следующим шагом на пути к диверсификации и развитию российского рынка ИБ видится выход на зарубежные рынки дружественных по отношению к России стран.

Подводя итоги оценки рынка ИБ стран Ближнего Востока и Северной Африки, стоит отметить, что на текущий момент ближневосточный рынок развит очень неравномерно. Преобладающее количество решений поставляется крупными международными корпорациями, стремящимися занять ключевые ниши на рынке продуктов ИБ не только в регионе, но и во всем мире. Ближневосточные страны с развитой экономикой, такие как Израиль, ОАЭ и Саудовская Аравия давно и очень активно развивают собственный рынок ИБ, инвестируя денежные средства не только в продукты и услуги, но и создавая условия для стабильного долгосрочного развития рынка. Правительство в этих странах осознает значимость создания благоприятных условий для привлечения инвестиций, поэтому в значительной степени упрощает и совершенствует законодательство, делая его более гибким и привлекательным для иностранных

вендоров. Страны Северной Африки, а также некоторые ближневосточные государства, имеющие низкие доходы на душу населения, начали вкладываться в развитие рынка ИБ относительно не так давно. Государственные органы в этих странах прикладывают усилия для цифровизации экономики, однако на текущий момент эти рынки не кажутся привлекательными для инвестирования, поскольку имеют слабое законодательство и высокие риски невозврата инвестиций. Зато Египет может быть привлекательны для российских компаний. Уже сейчас можно наблюдать неподдельный интерес к российским решениям в области кибербезопасности.

Список литературы

1. Актуальные киберугрозы: итоги 2022 года (2023) // Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (дата обращения: 26.01.2023).
2. Алжир готовится стать «Меккой стартапов» Euronews по-русски // YouTube. 5 сентября 2022 г. URL: https://www.youtube.com/watch?v=Kz1gLicYccc (дата обращения: 29.03.2023).
3. Бекишев Ю.А., Куликов Д.А., Писаренко Ж.В. Риски кибератак на предприятия, входящие в реальный сектор экономики стран // Московский экономический журнал. 2022. № 4. С. 616-626.
4. Викторова Н. В Дубае создали венчурный фонд для поддержки стартапов // Деловые Эмираты. 2022. 29 апр. URL: https://www.businessemirates.ae/news/uae-property-news/v-dubaye-sozdali-venchurnyy-fond-dlya-podderzhki-startapov/ (дата обращения: 29.03.2023).
5. В Алжире заработала система электронных платежей // Информационное агентство REGNUM. 2021. 24 дек. URL: https://regnum.ru/news/polit/3461239.html (дата обращения: 04.04.2023).
6. Гальцев А. Пустыня единорогов: как не провалить вывод стартапа в арабскую Кремниевую долину // Forbes. 2022. 29 июля 2022 URL: https://www.forbes.ru/mneniya/472791-pustyna-edinorogov-kak-ne-provalit-vyvod-startapa-v-arabskuu-kremnievuu-dolinu (дата обращения: 29.03.2023).
7. Города будущего против чековых книжек: опыт цифровизации разных стран (2022) // Платформа «vc.ru». 2022. 4 февр. URL: https://vc.ru/zyfra/359848-goroda-budushchego-protiv-chekovyh-knizhek-opyt-cifrovizacii-raznyh-stran?ysclid=lgjbi8z0ux142525965 (дата обращения: 29.03.2023).
8. Демидов П. Руководство по импортозамещению систем информационной безопасности в условиях санкций против России // Anti-Malware.ru. 2022. 11 апр. URL: https://www.anti-malware.ru/analytics/Market_Analysis/InfoSec-Systems-Substitution-Guide (дата обращения: 26.01.2023).
9. Дрожжин А. Ограбление XXI века: группировка хакеров Carbanak похитила миллиард долларов // Блог Касперского. 2015. 16 февр. URL: https://www.kaspersky.ru/blog/billion-dollar-apt-carbanak/6950/?ysclid=lh2fobo99w952075906 (дата обращения: 06.02.2023).
10. Дубай // TAdviser. 2023. 10 янв. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%94%D1%83%D0%B1%D0%B0%D0%B9 (дата обращения: 06.02.2023).
11. Египту представили российские ИТ-решения (2021) // Сайт Министерства цифрового развития, связи и массовых коммуникаций РФ 2021 URL: https://digital.gov.ru/ru/events/41363/ (дата обращения: 06.02.2023).
12. Информационная безопасность (рынок России). Обзор TAdviser «Безопасность информационных систем» (2023) // TAdviser URL: https://www.tadviser.ru/index.php/%D0%

A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_(%D1%80%D1%8B%D0%BD%D0%BE%D0%BA_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8)?ysclid=lgi59hicmm747381603 (дата обращения: 21.03.2023).

13. Исследование рынка информационной безопасности в России по клиентским сегментам (2022) // Ростелеком Солар URL: https://rt-solar.ru/upload/iblock/962/b7wyn7498evdp1jf8t7iccj5239ug4i9/Issledovanie-rynka-IB-RF-2022.pdf?ysclid=lh2gf1l5kg610937937 (дата обращения: 21.03.2023).

14. Кибернация Израиля (2018) // Softline URL: https://softline.ru/about/blog/kibernatsiya-izrailya?ysclid=lgrwq54qw7501485421 (дата обращения: 14.02.2023).

15. Королев Н., Литвиненко Ю. Выручка «ИКС Холдинга» по итогам 2022 года выросла до 91 млрд рублей // Коммерсантъ. 2023. 16 апр. URL: https://www.kommersant.ru/doc/5926558?ysclid=lge2lyhylc610486027 (дата обращения: 29.04.2023).

16. Крупнейшие компании России в сфере защиты информации. Обзор CNews Security: Информационная безопасность (2022) // Рейтинг сетевого издания Cnews URL: https://www.cnews.ru/reviews/security2022/review_table/12b4f5538e57db6abd0a5e202c744bc94f1ec876?ysclid=lh2ge2kr3u433713370 (дата обращения: 29.04.2023).

17. Лермонтова М. Новые возможности для запуска стартапов в ОАЭ. «Hub 71» // InternationalWealth.info. 2019. 27 сент. URL: https://internationalwealth.info/startups-abroad/new-opportunities-for-launching-startups-in-the-uae-hub-71/?ysclid=lgie35343j923786239 (дата обращения: 27.02.2023).

18. Оценка потенциала российских решений в области кибербезопасности на международном рынке (2022) // Центр стратегических разработок URL: h9lkrjgaawtho0hg7sy7ofgur7p9anx1.pdf (csr.ru) (дата обращения: 25.01.2023).

19. Прогноз развития рынка кибербезопасности в Российской Федерации на 2022–2026 годы (2022) // Центр стратегических разработок URL: Режим доступа: ufleu9rg5zc3ldu66srqt3a89j0mrve5.pdf (csr.ru) (дата обращения: 26.01.2023).

20. Softline значительно усиливает свое присутствие на Ближнем Востоке и в Африке за счет приобретения компании Seven Seas Technology, продолжая расширять свое глобальное присутствие (2022) // Softline URL: https://softline.ru/about/news/softline-significantly-bolsters-middle-east-and-africa-presence-through-acquisition-of-seven-seas-technology-continuing-to-expand-its-global-footprint?ysclid=lge1dlxnra19965113 (дата обращения: 06.02.2023).

21. Технологическая экосистема Израиля (2022) // Сайте Торгово-Экономического Представительства Посольства Государства Израиль в Москве URL: https://itrade.gov.il/russia/t%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F-%D1%8D%D0%BA%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0-%D0%B8%D0%B7%D1%80%D0%B0%D0%B8%D0%BB%D1%8F-%D0%BE/# (дата обращения: 12.02.2023).

22. Egypt FinTech Landscape Report (2021) // Central Bank of Egypt URL: https://enterprise.press/wp-content/uploads/2022/02/Egypts-FinTech-Landscape-Report-2021.pdf (date of treatment: 11.01.2023).

23. Fintech Development in Algeria Lags Behind MENA Counterparts (2021) // Fintech News Network URL: https://fintechnews.ae/8557/algeria/fintech-development-in-algeria-lags-behind-mena-counterparts/ (date of treatment: 15.03.2023).

24. Fintech in Algeria (2022) // Fintech Development in Algeria. URL: https://fintechinalgeria.com/ (date of treatment: 15.03.2023)

25. IMD World Digital Competitiveness Ranking (2021) // IMD World Competitiveness Center URL: https://www.tadviser.ru/images/f/f6/Digital_2021.pdf (date of treatment: 21.04.2023).

26. Israeli Cyber Security Industry Continued to Grow in 2021: Record of $8.8 Billion Raised (2022) // Israeli government. URL: https://www.gov.il/en/departments/news/2021cyber_industry (date of treatment: 22.04.2023).

27. Metinko C. VC Funding for Cybersecurity Companies in Israel on Pace to Nearly Double This Year (2023) // Crunchbase News. URL: https://news.crunchbase.com/news/israel-cybersecurity-startups-vc-investment/ (date of treatment: 29.03.2023).

PROSPECTS OF THE EXPORT OF RUSSIAN PRODUCTS AND SERVICES IN THE FIELD OF INFORMATION SECURITY. NEW MARKETS AND OPPORTUNITIES UNDER SANCTIONS PRESSURE (ON THE EXAMPLE OF ASSESSING INFORMATION SECURITY MARKETS IN THE MIDDLE EAST AND NORTH AFRICA)

Anastasiya Khusainova - Student of the optional course "GR in contemporary Russia: Theory and Practice", Department of the Theory and Practice of Business-Government Interaction, National Research University Higher School of Economics. Email: anastasia.khusainova.26@yandex.ru

Sergey Mytenkov - Senior Lecturer, Department of the Theory and Practice of Business-Government Interaction, National Research University Higher School of Economics. Vice President - Managing Director of the Regional Development Department of the Russian Union of Industrialists and Entrepreneurs. Ph.: +7 (495) 663 04 04 (ext. 1150)

This article is devoted to assessing the state of the information security market in the Russian Federation in relation to the financial sector of the Russian economy. The article provides an assessment of the export potential of Russian products and services in the field of cybersecurity in the Middle East and North Africa.

The significance and applied value of the study consists in the relevance of the problem considered by the authors. In the conditions of strict sanctions pressure and increasing competition in the domestic market, the management of Russian companies developing products and providing services in the field of information security is faced with the task of identifying the most promising foreign sales markets from the point of view of diversification. The authors pay special attention to the assessment of the current state of cybersecurity markets and the development of the financial sector in the Middle East and North Africa region.

Keywords:

cybersecurity, information security, financial sector, export potential, Middle East, North Africa.