УДК 528.71
DOI 10.33764/2618-981X-2023-6-263-267

Д. Л. Фишев[1], С. Н. Новиков[1,2]*

Анализ и оценка ситуации на рынке информационной безопасности в условиях санкционного давления на Российскую Федерацию

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
[2] Сибирский государственный университет телекоммуникаций и информатики, г. Новосибирск, Российская Федерация
* e-mail: dvs2954@mail.ru

Аннотация. Данная статья рассматривает текущую ситуацию на рынке информационной безопасности в России в условиях санкционного давления на страну. Анализируются основные вызовы, стоящие перед российскими компаниями в области информационной безопасности, и делается вывод о необходимости разработки эффективных мер по защите информации. Одним из основных трендов является увеличение спроса на услуги по защите данных и информации, но вызовы связаны с отсутствием квалифицированных специалистов в этой области и недостаточным развитием рынка информационной безопасности. В статье предлагается ряд рекомендации по улучшению ситуации с отсутствием квалифицированных специалистов и по исправлению ситуации недостаточного развития российского рынка информационной безопасности. В целом, статья является актуальной и полезной для понимания текущей ситуации на рынке информационной безопасности в России.

Ключевые слова: информационная безопасность, анализ статистических данных, SWOT-анализ

D. L. Fishev[1], S. N. Novikov[1]*

Analysis and Assessment of the Situation on the Information Security Market in the Context of Sanctions Pressure on the Russian Federation

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
[2] Siberian State University of Telecommunications and Informatics, Novosibirsk, Russian Federation
* e-mail: dvs2954@mail.ru

Abstract. This article examines the current situation in the information security market in Russia under sanctions pressure on the country. The main challenges facing Russian companies in the field of information security are analyzed, and a conclusion is made about the need to develop effective measures to protect information. One of the main trends is an increase in demand for data and information protection services, but the challenges are related to the lack of qualified specialists in this field and insufficient development of the information security market. The article offers a number of recommendations to improve the situation with lack of qualified specialists and to remedy the situation with insufficient development of Russian information security market. In general, the article is relevant and useful for understanding the current situation on the information security market in Russia.

Keywords: information security, statistical data analysis, swot-analysis

Введение

В результате беспрецедентного санкционного давления на Российскую Федерацию вопросы информационной безопасности (далее – ИБ) становятся еще более актуальными. Шквал кибератак и утечки данных могут нанести значительный ущерб как государству, так и отечественным компаниям в целом. Поэтому для разработки эффективных мер по защите информации необходимо проанализировать и оценить рынок ИБ. В данной статье мы проанализируем текущее состояние рынка ИБ на фоне влияния санкций на Российскую Федерацию и рассмотрим основные вызовы, которые стоят перед российскими компаниями в области ИБ.

Методы и материалы

Для анализа и оценки состояния рынка ИБ под давлением санкции против Российской Федерации были использованы следующие научные методы:

1) анализ статистических данных. Были обобщены и проанализированы данные о количестве кибератак и обнаружений уязвимостей программного обеспечения на российскую информационную инфраструктуру (рис. 1);

2) SWOT-анализ. Для определения сильных и слабых сторон российского рынка ИБ, а также возможностей и угроз был проведен SWOT-анализ (табл. 1). Исследования основываются на анализе статей крупных информационно-аналитических компаний, специализирующихся на вопросах ИБ [1 – 3].

Результаты

Анализ статистических данных показал, что с момента начала специальной военной операции в 2022 году количество инцидентов увеличилось на 80 %. Порядка 98 % веб-приложений подвержены кибератакам, утечки данных выявлены в 90 % приложений [1, 4]. Кибератаки направлены на информационную инфраструктуру как в частном, так и в государственном секторах. Так, каждая четвертая компания потеряла от них от 1 млн. до 500 млн. рублей. При мониторинге инцидентов кибератак в России показатели с каждым кварталом увеличиваются [5].

В нынешней ситуации санкции, наложенные англосаксонским миром на Российскую Федерацию, привели к серьезным проблемам ИБ для российских компаний. В частности, многие западные компании, работавшие в России, перестали оказывать услуги отечественным компаниям, что привело к определенному дефициту [6]. В этой связи отечественные компании были вынуждены обратиться к российским разработчикам решений и поставщикам услуг ИБ. Отметим, что российские компании не всегда готовы предоставить потребителям высококачественные услуги сферы ИБ. Это объясняется тем, что наш, отечественный рынок решений в сфере ИБ все еще не развит достаточно хорошо, что отчасти объясняется отсутствием квалифицированных специалистов в данной области [7].

Как указано выше, одной из основных проблем российского рынка ИБ является нехватка квалифицированных специалистов в этой области. В результате многие компании-потребители услуг ИБ не могут должным образом защитить

свою информацию. Также огромной проблемой для российского рынка ИБ является недостаточное развитие инфраструктуры. Это факт приводит к тому, что многие отечественные компании вынуждены посредством серого импорта обращаться к западным поставщикам услуг сферы ИБ, что является проблемой в нынешних условиях.

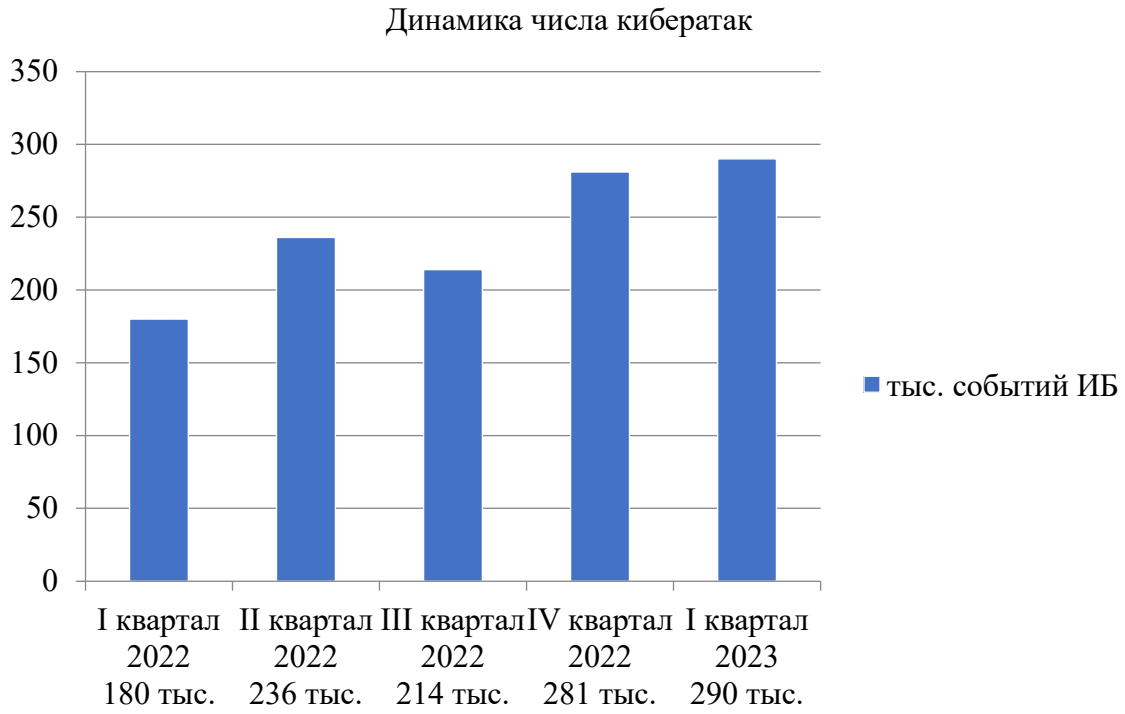

Рис. 1. Сводная статистика по событиям кибертатак

Таблица 1

SWOT-анализ для выявления сильных и слабых сторон российского рынка ИБ

Сильные стороны:	Слабые стороны:
– высокий уровень технической экспертизы и компетенции в области кибербезопасности; – наличие крупных компаний, специализирующихся на ИБ; – наличие сильных технических университетов и научных центров, занимающихся проблемами ИБ.	– нехватка квалифицированных специалистов по ИБ; – не достаточно хорошо развита инфраструктура для обеспечения ИБ; – недостаточная государственная поддержка отрасли; – отсутствие финансирования и инвестиций в отрасль.
Возможности:	Угрозы:
– рост спроса на услуги по обеспечению ИБ в связи с увеличением количествакибератак и угроз; – развитие новых технологий в области кибербезопасности.	– санкции и ограничения на международное сотрудничество; – усиление кибератак и угроз из-за рубежа и киберпреступников; – недостаточная осведомленность пользователей о необходимости обеспечения ИБ.

Для решения проблемы дефицита квалифицированных специалистов на рынке ИБ первым шагом следует провести унификацию образования в России, то есть выход из Болонской системы высшего образования. Тем самым будущее за нашей собственной уникальной системой образования, в основе которой будет лежать интересы национальной экономики и безопасности. Вторым шагом следует рассмотреть вопрос увеличения бюджетных ассигнований федерального бюджета, тем самым разработать и нарастить количество профильных образовательных программ, чтобы готовить различных экспертов, а не одинаковых кадров. Также можно увеличить возможность получения образования на коммерческой основе за счет средств предприятий и организаций. Третьим шагом следует рассмотреть вопрос, чтобы у новых специалистов появилась заинтересованность в сфере ИБ. Для этого привлекать экспертов ведущих компаний по ИБ читать лекции и рассказывать о деятельности компаний, выдавать гранты на обучение с возможностью стажировки и предоставлением рабочих мест после окончания университетов. Четвертым шагом в этом вопросе стоит рассмотреть возможность улучшения условии труда путем увеличения заработной платы.

Также оценивая рынок ИБ России в настоящее время, для его развития следует продумать вопросы поддержки отечественных компаний, чтобы у них была возможность развивать свои новые технологии, тем самым сделать их конкурентоспособными на мировом рынке [8]. С уходом зарубежных компаний освободились ниши, которые теперь могут занять российские компании [9]. Важно также укреплять законодательство в сфере ИБ, чтобы защитить права и интересы пользователей и компаний. При этом необходимо создавать специальные законы.

Цель данных мер заключается в том, чтобы достичь большого прогресса в защите информации и в борьбе с киберугрозами на территории Российской Федерации.

Заключение

Таким образом, можно сделать следующие выводы, что основной тенденцией российского рынка ИБ является рост спроса на услуги по защите информации. Однако проблемами являются дефицит квалифицированных специалистов и неразвитость российского рынка ИБ.

В целом, для развития российского рынка ИБ необходимо принять ряд мер, которые будут направлены на создание благоприятной среды для развития компаний, повышение квалификации специалистов, расширение научно-исследовательской базы, поддержку государства и укрепление законодательства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Актуальные киберугрозы: итоги 2022 года. – Текст: электронный //Российская компания, специализирующаяся на разработке решений в сфере информационной безопасности: [ptsecurity.com] – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (дата обращения: 05.05.2023).

2. Информационная безопасность (рынок России). – Текст: электронный // Портал выбора технологий и поставщиков: [www.tadviser.ru]. – URL:https://www.tadviser.ru/in-

dex.php/Статья:Информационная_безопасность_(рынок_России)?ysclid=lhk98voole825367744 (дата обращения: 05.05.2023).

3. Анализ российского рынка информационной безопасности. – Текст: электронный // Независимый российский информационно-аналитический центр: [anti-malware.ru.] - URL: https://www.anti-malware.ru/analytics/Market_Analysis/Russian-InfoSec-Market/ (дата обращения: 05.05.2023).

4. ТАСС: информационное агентство России: [www.tass.ru]. – Москва, 1999 –URL: https://tass.ru/ekonomika/15562907?ysclid=lhk8w4dtk3645727213 (дата обращения: 05.05.2023). – текст: электронный.

5. Кибератаки на российские компании 1 квартал 2023 года. – Текст: электронный//Комплекссервисов для защиты каналов связи, защиты от угроз кибербезопасности: [rt-solar.ru] - URL:https://rt-solar.ru/upload/iblock/ad3/3j9s24qws3lcnjmoilaowut9afff7jco/Otchet-Kiberataki-na-rossiyskie-kompanii-v-I-kvartale-2023-goda.pdf?ysclid=lhk3th3pbq873211372 (дата обращения: 05.05.2023).

6. Едакин А. Какие интернет-компании ушли из России? Последствия и альтернативы. - Тест: электронный // Тендерная площадка: [Workspace.ru] – URL: https://workspace.ru/blog/exodus-of-companies/ (дата обращения: 06.05.2023).

7. Гиацинтова С.Т. Актуальные аспекты управления персоналом в IT-компаниях // Управление человеческим потенциалом. – 2009. – № 2. – с. 146-149.

8. Постановление Правительства РФ от 06.04.2022 №598 «О внесении изменений в Правила предоставления субсидии из федерального бюджета Российскому фонду развития информационных технологий на поддержку проектов по разработке и внедрению российских решений в сфере информационных технологий». Правительство РФ. – текст: электронный.

9. Аллуш Мухамед Фехд. Влияние санкций на рынок ИТ // Материалы IX Международной студенческой научной конференции. Студенческий научный форум. - (дата обращения: 10.05.2023). – текст: электронный.