Вестник Тверского государственного университета. Серия: Экономика и управление. 2019. №3 (47). С. 162–168.

УДК 338.46

ОСОБЕННОСТИ ФОРМИРОВАНИЯ И ОСНОВНЫЕ ЧЕРТЫ РЫНКА УСЛУГ ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ НА СОВРЕМЕННОМ ЭТАПЕ

Д.С. Вахрушев[1], Н.И. Липовская[2]

[1,2]Ярославский государственный университет им. П.Г. Демидова, Ярославль

Цель статьи – анализ тенденций развития рынка услуг по обеспечению кибербезопасности на современном этапе. Актуальность данной проблематики обусловлена современными тенденциями развития информационного общества, сопровождающимися существенным возрастанием рисков обеспечения безопасности информационных систем практически во всех сферах и сегментах экономических отношений. Показано, что в результате постоянного роста спроса на данные услуги формируется и динамично развивается особый рынок, характеризующийся рядом специфических черт. Сформулирован вывод о том, что рынок услуг по обеспечению кибербезопасности в основном развивается по модели рынка монополистической конкуренции с чертами олигополистического рынка. При этом формирование адекватной модели рынка будет в значительной степени влиять на уровень трансакционных издержек в экономической системе и во многом детерминировать динамику экономического развития как бизнес-структур различного уровня, так и государства в целом.

Ключевые слова: *кибербезопасность, информационная безопасность, рынок услуг, неценовая конкуренция.*

Одной из наиболее заметных и привлекающих к себе внимание в последние десятилетия тенденций выступает глобальная информатизация общества. В конце XX в. зародилось исторически новое явление – информационная экономика, с ее отличительными чертами, приоритетами и новым типом экономического роста. Укоренившись как господствующий вектор постиндустриального развития, информационная экономика оказывает доминирующее влияние на все сферы социально-экономической жизни общества. При этом, наряду с безусловно положительным воздействием на динамику хозяйственных процессов, информатизация также генерирует новый класс рисков (информационные риски). Обеспечение информационной безопасности становится объективной необходимостью во всех сферах и сегментах экономических отношений, что обуславливает активное развитие нового рынка – рынка услуг по обеспечению кибербезопасности.

Термин «кибербезопасность» появился еще в начале XXI в., но по-прежнему его можно назвать новым. В настоящее время можно говорить о том, что услуги по обеспечению прозрачности и безопасности сети являются актуальными для всех секторов экономики, независимо от сферы и масштабов функционирования. При этом своеобразным предшественником термина «кибербезопасность» является часто употребляемое понятие «информационная безопасность», которое имеет более широкое определение. В этой связи обратим внимание на тот факт, что информационная безопасность включает в себя не «кибер-» и «оффлайн-» информацию, то есть, она связана не только с

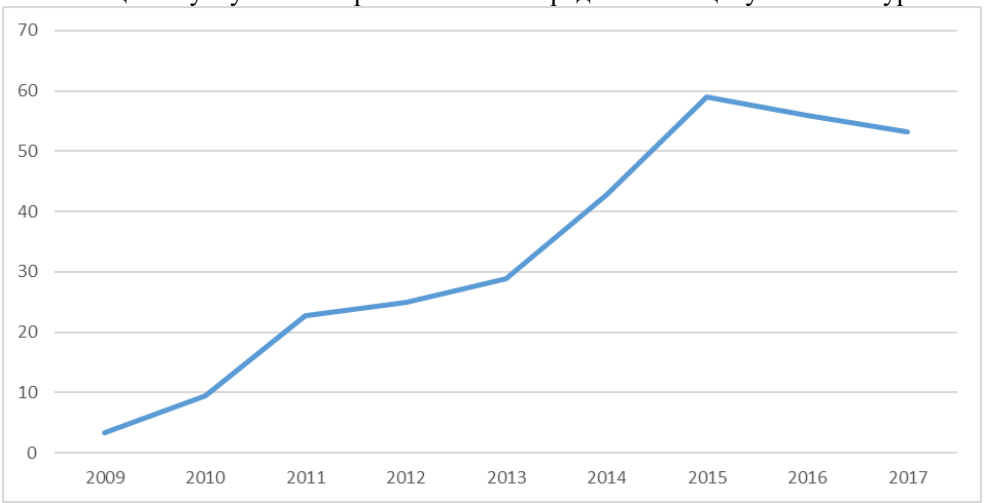
компьютерными данными, источниками и хранилищами. Определение «информационной безопасности» варьируется, но всегда сосредоточено на защите конфиденциальности, целостности, полноты, доступности информации вне зависимости от ее формы.

Кибербезопасность в определении, данном в 2011 г. консалтинговой компанией PwC, подразумевает разработку продуктов и услуг для противостояния «агрессивным» приложениям, то есть, различного рода кибер-атакам, с уточнением, что данные услуги наиболее актуальны для государственного и военного секторов, а также используются в виде кибер-оружия или кибер-защиты. Вторая часть определения говорит о том, что кибербезопасность имеет место не только там, где речь идет об Интернет-протоколах или устройствах, подключенных к сети Интернет, но это также присуще телеком-оборудованию и промышленному оборудованию [1].

В настоящее время субъектами рынка кибербезопасности являются компании, которые предоставляют продукты и услуги по обеспечению защиты от различного вида кибер-угроз в сфере информационных технологий (ИТ), телекоммуникаций, промышленности, транспорта, банковского дела, образовательного сектора и др., причем масштабы рынка кибербезопасности продолжают увеличиваться. Подобная тенденция сохраняется с 2009 г. По нашему мнению, высокие темпы роста данного рынка в значительной мере обусловлены эффектом «низкой базы», то есть, его новизной и неразвитостью в предшествующие периоды. В то же время, по мере дальнейшего развития, сокращение темпов роста анализируемого рынка представляется вполне закономерным.

Методологически анализ динамики темпов роста того или иного рынка должен опираться на доминирующие индикаторы. Представляется, что ключевым индикатором масштабности развития рынка кибербезопасности служит динамика расходов, осуществляемых потребителями на обеспечение защиты от агрессивных действий в информационной среде. Весьма показательными в этом смысле выступают следующие данные: в 2017 г. расходы на кибербезопасность составили 86,4 млрд долл. США, по сравнению с 60 млрд долл. США в 2011 г. Тем самым, на протяжении всего промежутка времени рост составлял порядка 15 % ежегодно [1, 2].

Очевидно, что данная тенденция также связана с развитием технологий. За последние годы Интернет-устройства стали очень мобильными, что потребовало от поставщиков услуг по кибербезопасности предлагать защиту на новых уровнях.



Р и с . 1. Количество зарегистрированных кибератак в 2009–2017 гг. в мире, млн

Однако вместе с тем растет количество кибератак и преступлений. Так, количество зарегистрированных кибер-атак в 2017 г. составило 53,3 млн, по сравнению с 2009 г. оно увеличилось в 15 раз (рис. 1). Ежегодно в течение рассматриваемого периода, вплоть до 2016 г., этот показатель увеличивался минимум на 30 % [5].

Наиболее уязвимыми, и в то же время привлекательными для кибер-преступлений отраслями, являются государственный сектор (по итогам 2017 г. в мире зарегистрировано 22 788 инцидентов), сфера развлечений (7 188 зарегистрированных инцидентов), информационные услуги и сфера ИТ (1 040 инцидентов), медицина и здравоохранение (750 инцидентов), финансовый сектор (598 инцидентов) (рис. 2). В меньшей степени кибератакам подвержены сферы недвижимости, образования, транспорта, розничной торговли, строительства, административных услуг и др. Данные по количеству кибератак представлены в табл. 1 и на рис. 2. Эта статистика включает только зарегистрированные инциденты.

Р и с . 2. Доля кибер-преступлений, зарегистрированных в различных сферах экономики за 2017 г., % от общего числа.

По мнению авторов, к главным факторам, влияющим на развитие рынка кибербезопасности, следует отнести:

– появление всё новых типов кибератак, основанных на новых угрозах и имеющих новые векторы развития;

– рост уязвимости, связанный со всё более широким использованием «облачных» технологий хранения и обмена данных;

– рост осведомленности компаний и потребителей о возможных угрозах безопасности сети;

– изменения технологий, определяющих состав продукта, а также появление инноваций, влияющих на решения по обеспечению безопасности сети;

– формирование законодательной базы, фиксирующей перечень требований по защите персональных данных;

– изменения в структуре организаций (часть компаний переводит функции отдела безопасности на аутсорсинг, в то время как другая часть выстраивает собственную иерархическую систему по обеспечению информационной безопасности предприятия на всех уровнях).

Кроме того, рассматривая формирование и развитие рынка кибербезопасности с позиции долгосрочной перспективы, можно выделить ряд движущих факторов из таких парадигм информационной экономики, как инфраструктура рынка, большие данные, количество подключенных пользователей, сфера финансов, Интернет, нормативно-законодательная база и др. Эти факторы также влияют и на сегментацию рынка. В этой связи рынок кибербезопасности может быть сегментирован по технологиям (в зависимости от того, какие задачи они решают) и по вертикали (секторам экономики). Рассмотрим подробнее эти варианты сегментации.

Решения по кибербезопасности призваны защищать сетевую инфраструктуру и все устройства, которые к ней подключены. По видам решений выделяются управление идентификацией и доступом (Identity and Access Management – IAM), управление рисками и требованиями, шифрование, предотвращение потери данных (Data Loss Prevention – DLP), унифицированное управление угрозами (Unified Threat Management – UTM), брандмауэр, антивирус/антивирусное ПО, система обнаружения вторжений / система предотвращения вторжений (Intrusion Detection System/Intrusion Prevention System – IDS/IPS), безопасность и управление уязвимостями, аварийное восстановление, смягчение объемных атак, связанных с отказом в обслуживании (Distributed Denial of Service – DDoS), веб-фильтрация и другие решения (включая управление белыми списками приложений и управление исправлениями) [3].

Сегментация рынка кибербезопасности по секторам экономики в настоящее время весьма обширна и включает в себя почти полный перечень. Можно отметить, что в секторе медицины и здравоохранения ожидается значительный рост инвестиций в область обеспечения кибербезопасности с 2018 по 2023 гг., поскольку информационные данные и цифровые устройства в этой сфере подвергаются значительному количеству кибератак. Кроме того, в сфере финансов, в банковском секторе, в сфере страхования, ИТ и телекоммуникаций также ожидается стремительный рост показателей масштабов рынка за рассматриваемый период.

Одним из важнейших этапов анализа рынка является уточнение его институционального состава. Критерии, по которым составляются рейтинги компаний по кибербезопасности, многообразны. Приведем список из 10 компаний-лидеров рынка по нахождению их в мировых рейтингах и по наличию у них клиентов в России: IBM (США), Symantec (США), Check Point (США), Cisco (США), F5 Networks (США), FireEye (США), Forcepoint (США), Juniper Networks (США), Palo Alto Networks (США), Flowmon Networks (Чехия).

На российском рынке крупнейшими производителями являются «Лаборатория Касперского», Positive Technologies, «Код безопасности» и «Инфотекс». При этом «Лаборатория Касперского» – единственная компания, которая входит в мировой рейтинг топ-10 поставщиков услуг в сфере кибербезопасности.

В России значимую роль играет фактор государственного регулирования рынка. Так, требования к поставщикам услуг по мониторингу и обеспечению безопасности сети очень высоки, производитель обязан пройти сертификацию и иметь все необходимые лицензии. Однако данное требование может стать

барьером для входа на рынок только для иностранных производителей. Ситуация осложняется за счет сильной конкуренции и государственной поддержки национальных производителей в сфере ИТ [4].

Обратимся теперь к анализу рынка услуг по обеспечению кибербезопасности с точки зрения конкурентных отношений. Думается, что данный рынок в большей степени соответствует модели рынка монополистической конкуренции, для которой характерна неценовая конкуренция. При этом сами услуги не универсальны, каждый производитель наделяет их уникальными характеристиками, что приводит к отсутствию на рынке совершенных товаров-заменителей. Каждая фирма занимает долю на рынке, которая не превышает 1–10 %. Цены на услуги обычно не оглашаются в масштабах деятельности рынка: каждый производитель устанавливает свою цену, которая, в зависимости от ряда критериев, может быть выше или ниже, чем у конкурентов. Однако это не является определяющим фактором при формировании стратегии. Наиболее значимо наличие у компаний-лидеров устоявшейся многолетней репутации и узнаваемости имени-бренда во всем мире. Для потребителей это зачастую имеет решающее значение при выборе поставщика услуг и для выстраивания отношения лояльности к бренду. В попытках превзойти друг друга в конкурентной борьбе производители привносят дополнительные характеристики к решениям, стремятся расширить ассортимент, повысить качество, использовать все новые НИОКР, увеличивать расходы на рекламу и гарантийное обслуживание. Их клиенты – как правило, компании крупного, среднего и малого бизнеса, государственные учреждения. Представители этих компаний – сотрудники подразделений по ИТ-безопасности, управляющие менеджеры, линейные исполнители, которые, в свою очередь, напрямую взаимодействует с представителями поставщика услуг. Тем самым в данных отношениях имеют место преференции, история сотрудничества, предлагаемые пакеты услуг и технической поддержки, что ставит важность стоимости услуг на второе место. Помимо этого, компании-поставщики используют значительную часть бюджета для целей маркетинга и рекламы, что включает в себя участие в тематических выставках и конференциях, проведение рекламных кампаний, спонсорство, поддержку университетских проектов и другие.

Таким образом, рынок кибербезопасности является частью рынка информационной безопасности, поскольку последний появился гораздо раньше и формировался изначально без влияния цифровых данных, особенностей хранения и обмена информацией в Интернете и облачных технологий. Объемы рынка кибербезопасности продолжают расти. В настоящее время кибер-угрозам подвержены все сферы экономики, они затрагивают как крупные, так и малые предприятия, не ограничиваясь государственным и военным сектором, как это было в 2008 г. Факторы развития рынка связаны с развитием технологий, формированием законодательной базы и изменениями в структурах корпораций. Важным фактором является государственная поддержка производителей услуг по обеспечению кибербезопасности. Сегментация исследуемого рынка во многом определяется вышеуказанными факторами и изменяется под влиянием развития технологий и появления новых областей применения решений по обеспечению прозрачности сети и ее безопасности. Главными игроками на данном рынке являются компании США, среди российских компаний в мировой рейтинг входит Лаборатория Касперского. Рынок кибербезопасности имеет черты рынка монополистической конкуренции и характеризуется преимущественным использованием неценовых методов, что влияет на определение конкурентных

стратегий компаний. Формирование адекватной модели рынка будет в значительной степени влиять на уровень трансакционных издержек в экономической системе и в значительной степени детерминировать динамику экономического развития как бизнес-структур различного уровня, так и экономики страны в целом.

Список литературы

1. PwC Cyber Security M&A review. November, 2011.
2. PwC /Technology Safety Board Information Security, 2020 report.
3. Cybersecurity Market worth $248.26 billion by 2023 – Агентство аналитических исследований Markets&Markets [Электронный ресурс]. – URL: https://www.marketsandmarkets.com/PressReleases/cyber-security.asp.
4. Жукова К. В кибербезопасности не велик выбор // Коммерсант. 2018. № 40. С. 5.
5. Global number of cyber security incidents from 2009 to 2015 (in millions) [Электронный ресурс]. – URL: https://www.statista.com/statistics/387857/number-cyber-security-incidents-worldwide/.
6. Global number of cyber security incidents in 2017, sorted by victim industry and organization size [Электронный ресурс]. – URL: https://www.statista.com/statistics/194246/cyber-crime-incidents-victim-industry-size/.

FORMATION PECULIARITIES AND KEY FEATURES OF CYBER SECURITY SERVICES MARKET AT THE PRESENT STAGE

D.S. Vakhrushev[1], N.I. Lipovskaia[2]

[1,2]Yaroslavl state University of P. G. Demidov, Yaroslavl

The paper explores key trends in the market for cybersecurity services at the present stage. The relevance of this issue is based on contemporary trends in the development of the information society accompanied by the significant increase in the risks of ensuring information systems security in almost all areas and segments of economic relations. As a result of the constant growth in demand for these services, a special market with a number of specific feature is forming and dynamically developing. The authors conclude that the market for cybersecurity services mainly develops according to the market model of monopolistic competition. At the same time, the formation of an adequate market model will significantly affect the level of transaction costs in the economic system and will largely determine the dynamics of economic development of both business structures at various levels and the state as a whole.

***Keywords**: cybersecurity, information security, non-price competition.*

Об авторах:

ВАХРУШЕВ Дмитрий Станиславович – доктор экономических наук, профессор кафедры финансов и кредита, Ярославский государственный университет им. П.Г. Демидова, e-mail: boxer204@mail.ru

ЛИПОВСКАЯ Наталья Игоревна – аспирант, Ярославский государственный университет им. П.Г. Демидова, e-mail: n.i.lipovskaya@gmail.com

About the authors:

VAHRUShEV Dmitrij Stanislavovich – PhD in Economics, Professor of Finance and credit, Yaroslavl state university of P. G. Demidov, e-mail: boxer204@mail.ru

LIPOVSKAJa Natal'ja Igorevna – Postgraduate student, Yaroslavl state university of P. G. Demidov, e-mail: n.i.lipovskaya@gmail.com

References

1. PwC Cyber Security M&A review November 2011.
2. PwC /Technology Safety Board Information Security 2020 report.
3. Cybersecurity Market worth $248.26 billion by 2023 – Agentstvo analiticheskih issledovanij Markets&Markets, - EHlektronnyj resurs, URL: https://www.marketsandmarkets.com/PressReleases/cyber-security.asp.
4. ZHukova K. V kiberbezopasnosti ne velik vybor // Kommersant. 2018. №40. str. 5.
5. Global number of cyber security incidents from 2009 to 2015 (in millions), - EHlektronnyj resurs, URL: https://www.statista.com/statistics/387857/number-cyber-security-incidents-worldwide/.
6. Global number of cyber security incidents in 2017, sorted by victim industry and organization size, - EHlektronnyj resurs, URL: https://www.statista.com/statistics/194246/cyber-crime-incidents-victim-industry-size/.