DOI 10.37882/2223-2974.2023.09.21

ОПТИМАЛЬНАЯ МОДЕЛЬ УПРАВЛЕНИЯ КОМПАНИЕЙ В СФЕРЕ ОБЕСПЕЧЕНИЯ КИБЕР И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Мартынюк Максим Сергеевич
Аспирант, Московский финансово-промышленный университет Синергия, г. Москва
take_over_control@mail.ru

Аннотация. В настоящее время отмечается процесс глобальной информатизации общества, что приводит к масштабным изменениям всех сфер экономики и появлению и развитию новых сегментов рынка. Так, одним из таких современных сегментов рынка является рынок услуг по обеспечению кибер и информационной безопасности. В связи с повышением уровня востребованности услуг данного сегмента рынка остро встает вопрос об оптимальном выстраивании управленческих процессов компаний в сфере обеспечения кибер и информационной безопасности. В статье представлены подходы к определению понятий «кибербезопасность» и «информационная безопасность», результаты анализа рынка информационной безопасности, особенности управления организацией в сфере кибер и информационной безопасности и оптимальная модель управления. Автор приводит к выводу о том, что для организаций в сфере кибер и информационной безопасности оптимальной является модель сервисного управления, которая позволяет сформировать конкурентные преимущества и предоставлять товары и услуги с опорой на клиентоориентированный подход.

Ключевые слова: кибербезопасность, информационная безопасность, модель управления, цифровизация, сервисное управление, информационная экономика.

OPTIMAL MODEL OF COMPANY MANAGEMENT IN THE FIELD OF CYBER AND INFORMATION SECURITY

M. Martynyuk

Summary. Currently, there is a process of global informatization of society, which leads to large-scale changes in all spheres of the economy and the emergence and development of new market segments. Thus, one of such modern market segments is the market of cyber and information security services. Due to the increasing demand for the services of this market segment, the question of optimal management processes of companies in the field of cyber and information security arises. The article presents approaches to the definition of the concepts of «cyber security» and «information security», the results of the analysis of the information security market, the peculiarities of organization management in the field of cyber and information security and the optimal management model. The author concludes that the optimal model for organizations in the field of cyber and information security is the service management model, which allows to form competitive advantages and provide goods and services based on a customer-oriented approach.

Keywords: cybersecurity, information security, governance model, digitalization, service management, information economy.

В последние годы глобальная информатизация общества как объект научных теоретических и прикладных исследований привлекает к себе все больше внимания. Это связано с тем, что в конце прошлого века зародилось новое явление — информационная экономика. Ее основными характеристиками и чертами стали: инновационный тип роста, цифровизация, расширение кибер и информационного пространства и т.д. Сегодня информационная экономика оказывает приоритетное влияние на все сферы социально-экономической жизни общества. Стоит отметить, что развитие и популяризация информационной экономики оказывает как положительное воздействие на динамику хозяйственных процессов, так и является следствием определенных негативных проявлений и проблем.

Как положительный фактор информационная экономика генерирует новые идеи, типы развития хозяйственных процессов, модели управления и взаимодействия определенных организаций. Как негативный фактор информатизация как обязательный процесс информационной экономики приводит к генерированию новых рисков, связанных с защитой и хранением информации. Кибер и информационные риски, их учет, преодоление и профилактика становятся объективной необходимостью во всех сегментах экономических отношений. Этот факт является причиной активного развития нового сегмента на рынке услуг — услуга по обеспечению кибер и информационной безопасности [4].

Обратимся к исследованиям Л.Б. Парфеновой, Д.С. Вахрушева и Н.И. Липовской. Авторами отмечено, что услуги по обеспечению информационной и кибербезопасности в настоящее время являются значимой частью инновационной инфраструктуры национальной экономики во всех странах. В контексте экономики России, которая находится на этапе развития цифрового сегмента, развитие этой инфраструктуры выступает в качестве важной национальной задачи. Во-первых, развитие сферы услуг по обеспечению кибербезопасности способствует общему развитию цифровой экономики, а во-вторых — защита информации в государственном и коммерческом секторах является условием для экономического функционирования производственных процессов различных организаций. Авторы выделяют следующие факторы, которые зави-

сят от состояния кибер и информационной безопасности предприятий [6]:

— эффективность и регулярность процессов предприятия;
— особенность работы различных структур предприятия;
— качество производимых и поставляемых предприятием услуг и товаров;
— качество оказываемых услуг конечным потребителям.

Соответственно, кибер и информационная безопасность — это важный фактор, который обуславливает устойчивость, надежность и функционирование экономических систем разного уровня и масштаба. Обеспечение кибер и информационной безопасности как объект проблемного вопроса интересует как производителей, так и потребителей во всех сегментах экономики.

Раскроем понятийный аппарат по поставленной проблеме. Так, определение кибербезопасности начало формироваться в начале нынешнего века, однако и на данный момент термин не имеет четкого определения и является достаточно новым. В настоящее время определение кибербезопасности корректируется в сторону того, что услуги по ее обеспечению являются востребованными во всех сегментах экономики. «Предшественником» термина «кибербезопасность» является понятие информационной безопасности, которое имеет более широкую трактовку. В научной литературе при определении термина «информационная безопасность» акцент делается на защите конфиденциальности и целостности информации, независимо от ее масштабов, назначения и формы [1].

Согласно определению, сформированному консалтинговой компанией PwC, кибербезопасность представляет собой разработку продуктов и услуг с целью противостояния агрессивным кибер-атакам разного рода. Консалтинговой компанией также уточняется, что данного рода услуги наиболее актуальны и востребованы в сфере военного и государственного секторов. При этом специалисты также отмечают, что о кибербезопасности речь идет также не только в контексте интернет-протоколов или технических устройств, но и в рамках обеспечения целостности и защищенности промышленного и телеком-оборудования [11, 12].

Для определения сущности кибер и информационной безопасности в России обратимся к Доктрине информационной безопасности РФ. Согласно вышеупомянутому нормативному акту, информационная безопасность представляет собой состояние защищенности личности, общества и государства от разного рода информационных рисков и угроз: внутренних, внешних и др. Обеспечение информационной безопасности — это обеспечение реализации прав и свобод человека в информационной среде [8].

Исходя из рассмотренных определений, можно отметить, что кибер и информационная безопасность как понятия включают в себя большое разнообразие проблем и, соответственно, решений. Субъектами рынка кибер и информационной безопасности выступаю компании, деятельность которых построена на предоставлении продуктов и услуг по обеспечению защиты и сохранности информации от различного рода угроз, кибератак и проблем. Эти компании реализуют свою деятельность в сфере информационных технологий, телекоммуникаций, промышленной сферы, транспортной сферы, банковского дела, сегмента образования и других видах и сферах деятельности. При этом каждый год рынок кибер и информационной безопасности растет, что можно связать с его новизной и неразвитостью. Соответственно, по мере дальнейшего развития рынка, по традиционным экономическим законам будет отмечаться сокращение темпов его роста, что приведет к необходимости модернизации и повышения конкурентоспособности компаний, реализующих свою деятельность в контексте этого рыночного сегмента.

Для оценки состояния рыка обратимся к методологии анализа динамики темпов роста рынка кибер и информационной безопасности с опорой на доминирующие индикаторы. Так, в рассматриваемом рыночном сегменте основным индикатором развития служит динамика расходов потребителей, то есть востребованность услуг по защите от кибератак и угроз. Согласно данным, представленным аналитической компанией Canalys, в сегменте обеспечения кибер и информационной безопасности затраты в 2022 году поднялись на 15,8 % (в сравнении с 2021 годом) и составили 71,1 млрд долларов. Аналитическая компания также оценила исследуемый сегмент рынка по шести ключевым позициям, таким как: средства обеспечения безопасности, инструменты сетевой защиты, безопасность данных, защиты электронной почты, веб-безопасность, анализ и поиск уязвимостей и системы управления доступа к данным. По мнению аналитиков, именно эти виды услуг станут наиболее востребованными, что скажется на ассортименте, масштабах и направленности компаний в сфере обеспечения кибер и информационной безопасности [5].

Для оценки и анализа рынка кибер и информационной безопасности уточним также его институциональный состав. Так, для данного направления анализа были просмотрены рейтинги компаний, которые осуществляют свою деятельность в данном сегменте рынка. По данным TAdviser, на конец 2022 года было выделено 12 ведущих компаний-поставщиков товаров, услуг и инструментов по обеспечению кибербезопасности. Название и доля рынка каждой компании представлены на рис. 1.

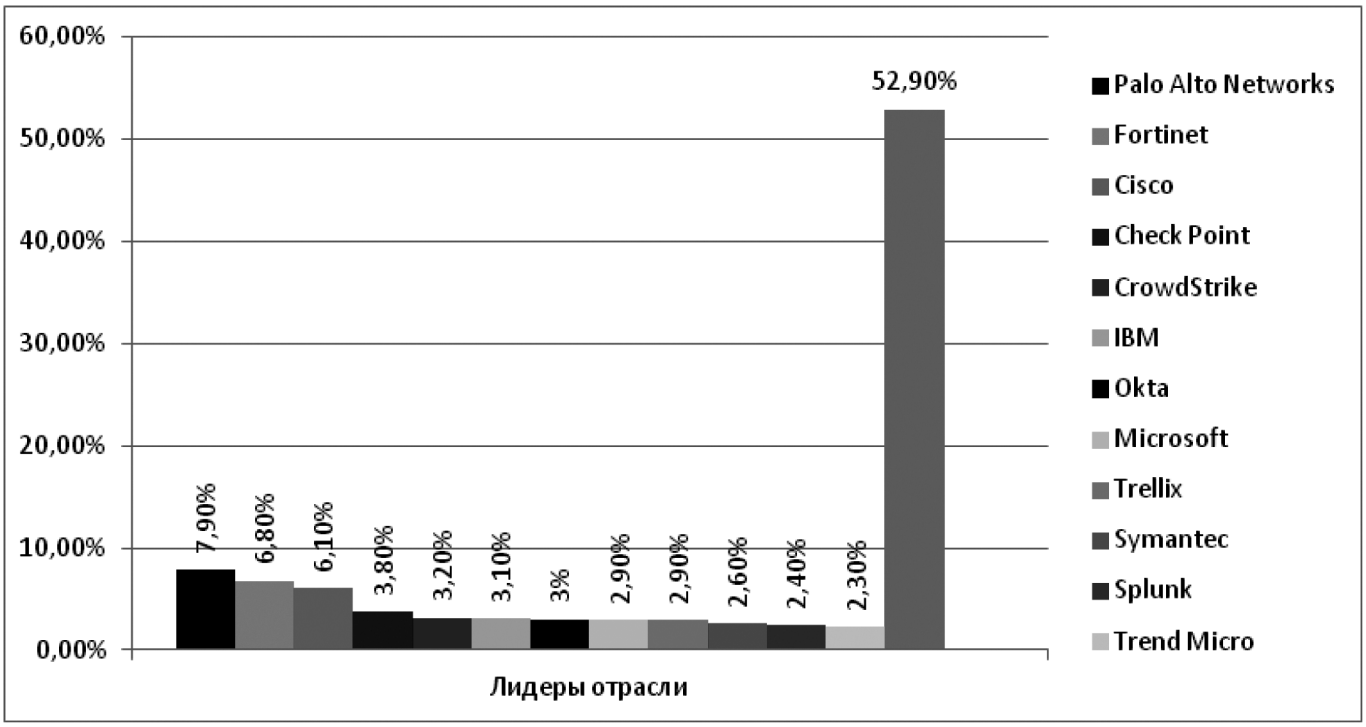

Рис. 1. Компании-лидеры рынка кибер и информационной безопасности на конец 2022 года
Источник: составлено автором на основе [5]

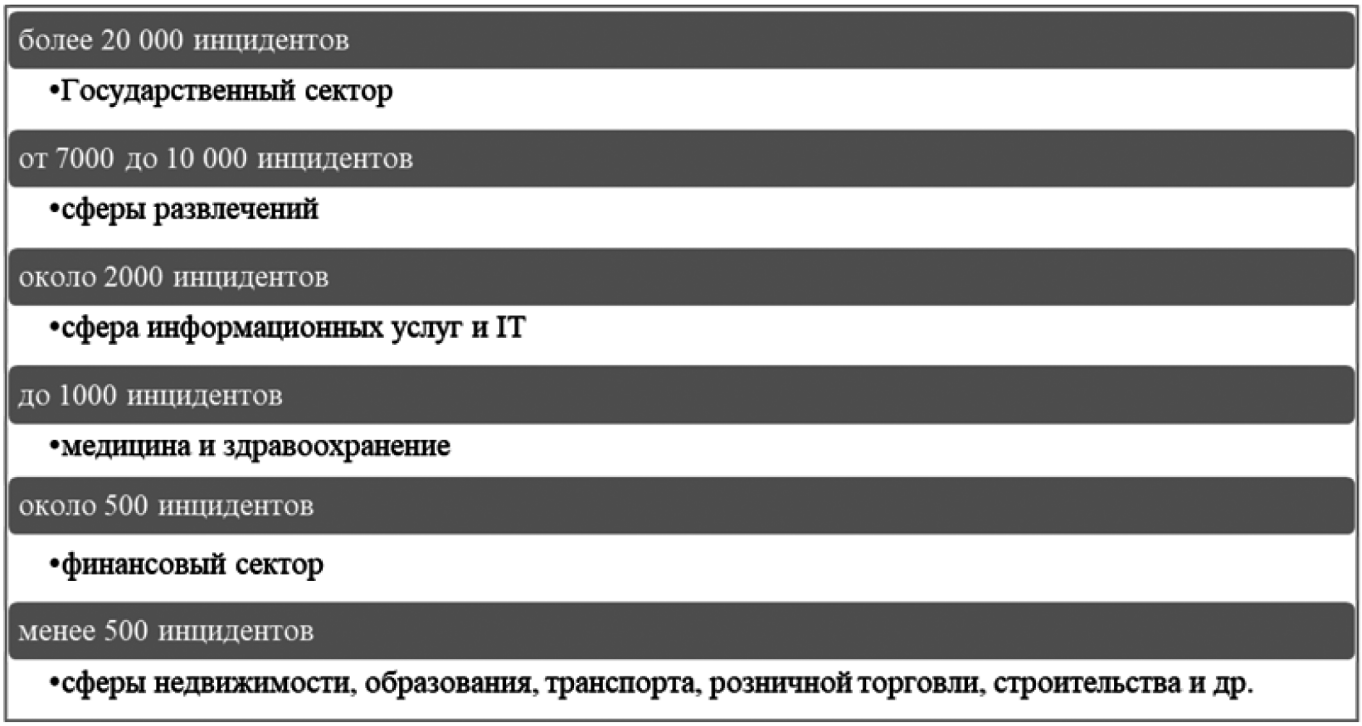

Рис. 2. Уязвимость различных секторов экономики по критерию среднего числа кибер-атак и угроз в год
Источник: составлено автором с опорой на [2]

Также, для анализа оптимальной модели управления компанией в рассматриваемом сегменте рынка важно проанализировать секторы экономики, в которых наиболее востребована услуга, оказываемая этими организациями. Как отмечают в своем исследовании Д.С. Вахрушев и Н.И. Липовская, практически во всех сферах экономики обеспечение кибер и информационной безопасности является важной и первостепенной задачей. Так, степень востребованности услуг по обеспечению кибер и информационной безопасности в различных сферах деятельности представлена на рисунке 2, составленном с опорой на среднее количество

кибератак и угроз как показателей уязвимости этой сферы.

Исходя из представленной на рисунке 2 информации можно сделать вывод о том, что наиболее уязвимые сферы выступают главными потребителями услуг в сфере кибер и информационной безопасности, что говорит о необходимости выстраивания модели управления организацией, осуществляющей деятельность в этой сфере, с опорой на удовлетворение потребностей и запросов этих сфер. Это также говорит о том, что обеспечение кибер и информационной безопасности является одной из главных задач ведущих сегментов рынка, и, соответственно, формирует запрос на развитие конкурентоспособных и клиентоориентированных компаний, которые смогут удовлетворить этот запрос.

К организациям, осуществляющим деятельность в сфере обеспечения кибер и информационной безопасности, предъявляются определенные требования, обусловленные значимой ролью государственного регулирования рынка услуг в данном сегменте. Так, к требованиям при осуществлении услуг по обеспечению кибер и информационной безопасности относят прохождение сертификации, высокий уровень технологичности, инновационность, наличие необходимых лицензий, результативность и качество поставляемых продуктов и услуг. Ориентируясь на соблюдение этих условий, многие организации в исследуемом сегменте рынка при построении модели управления делают упор на организационно-технические внутренние структуры и их развитие для удержания позиций в искусственно ограниченной конкурентной среде, что соответствует модели управления, ориентированной на обеспечение непрерывности бизнес-процессов [3].

Анализ специфики рынка услуг по обеспечению кибер и информационной безопасности позволяет отметить, что характерной для данного сегмента является модель рынка монополистической конкуренции с чертами олигополистического рынка. Такой модели соответствует преимущественно неценовая конкуренция. При универсальности услуг по обеспечению кибер и информационной безопасности, каждая организация сама устанавливает цену, которая, в зависимости от уникальных характеристик и критериев поставляемых товаров и услуг, может быть выше или ниже, чем у конкурентов. Соответственно, ценовая политика не является конкурентным преимуществом компании сферы кибер и информационной безопасности [6].

Для анализа наиболее оптимальных конкурентных преимуществ, которые необходимо учитывать при построении модели управления компанией в сфере обеспечения кибер и информационной безопасности, важно уточнить, что данный сегмент рынка является частью рынка услуг. При этом для рынка услуг характерна значимость такого конкурентного преимущества, как положительная репутация и узнаваемость бренда, так как эти факторы зачастую являются определяющими при выборе компании потребителями услуг. Также, высокая конкурентность, которая характерна для рынка информационной безопасности ввиду его активного развития и увеличения доли востребованности услуг, требует учета дополнительных характеристик помимо качества, технологичности и инновационности. Соответственно, формирование бренда, четкого позиционирования и создание клиентоориентированной концепции позволит повысить конкурентоспособность компании данной сферы.

Е.С. Янковская отмечает, что в условиях цифровизации экономики происходит усложнение механизмов взаимодействия участников рынка. По мнению автора, в настоящее время для управления процессами компании инновационных сфер (какой является сфера обеспечения кибер и информационной безопасности) необходимо учитывать следующие факторы [10]:

— управление должно быть нацелено на результат, на который настраивается вся система компании;
— управление должно выстраиваться на четких измеряемых задачах и целях;
— вся система компании должна сводится к одному — удовлетворение нужд и запросов потребителей, то есть управление должно выстраиваться с учетом клиентоориентированного подхода.

Соответственно, с учетом стремительного развития рынка информационной безопасности и расширения влияния организаций данного сегмента, значимым является определение оптимальных путей и моделей управления компанией в сфере обеспечения кибер и информационной безопасности. Под моделью управления подразумевается процесс, включающий в себя различные элементы, такие как организационная структура, корпоративная культура, политика компании и т.д. Среди традиционных подходов к управлению организацией можно выделить линейно-функциональную модель, директивную модель, матричную модель, модель ориентации на бизнес-процессы компании, сервисную модель и т.д. [9].

С учетом специфики услуг по обеспечению кибер и информационной безопасности, способствовать повышению конкурентоспособности предприятий данной сферы может сервисная модель управления, которая получила свое активное развитие в 2020 году, с приходом в «жизнь» компаний разных сфер пандемии и последствий распространения коронавирусной инфекции. Так, в основе этой модели лежит концепция «производим-продаем». Иными словами, заказчик получает у организации с сервисным подходом к управлению набор

услуг и/или товаров, а не конкретного специалиста. Примером таких услуг является техническая поддержка бизнес-приложений, непрерывная работа серверов, услуги по обеспечению кибер и информационной безопасности. Суть данной модели заключается в том, что заказчик не погружается в определенную специфику и нюансы услуг, при этом эти услуги реализуются компанией-поставщиком обезличено, по заранее оговоренным параметрам. Работа компании в сфере кибер и информационной безопасности с таким подходом — это гарантия безопасности, конфиденциальности, упрощения процесса сделки/продажи [7].

Можно констатировать, что сервисная модель управления организацией — это клиентоориентированный подход, который позволяет наиболее оптимально реализовать комплекс услуг компанией в сфере обеспечения кибер и информационной безопасности за счет согласования с бизнесом любой сферы таких параметров, как сроки, цена, диапазон воздействия, качество и т.д. Также, услуги, предоставляемые организацией с сервисной моделью управления, имеют понятное ценообразование (фиксированная цена за товар или услугу в определенные временной период) и гарантию качества на предоставляемые услуги.

Таким образом, можно сделать вывод о том, что рынок услуг по обеспечению кибер и информационной безопасности неуклонно развивается, что приводит к повышению уровня конкуренции в данном сегменте, а также к ужесточению требований, предъявляемых к организациям, осуществляемым деятельность в этой сфере. В связи с этим значимой становится проблема определения оптимальной модели управления для организаций в сфере кибер и информационной безопасности. Одной из таких моделей является сервисно-ориентированная модель управления, которая за счет параметров организации деятельности в компании позволяет производить услуги в сфере кибер и информационной безопасности, отвечающие запросам качества, понятной политики ценообразования и клиентоориентированности.

ЛИТЕРАТУРА

1. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность //Вопросы кибербезопасности. — 2014. — № 5 (8). — С. 39–42.
2. Вахрушев Д.С., Липовская Н.И. Особенности формирования и основные черты рынка услуг по обеспечению кибербезопасности на современном этапе // Вестник Тверского государственного университета. Серия: Экономика и управление. — 2019. — № 3. — С. 162–168.
3. Жукова, К.В кибербезопасности не велик выбор / К. Жукова // Коммерсант. 2018. — № 40. — С. 5.
4. Згоба А.И., Маркелов Д.В., Смирнов П.И. Кибербезопасность: угрозы, вызовы, решения //Вопросы кибербезопасности. — 2014. — № 5 (8). — С. 30–38.
5. Информационная безопасность (мировой рынок) / Tadviser, 2023 [Электронный ресурс]. URL: https://www.tadviser.ru/a/275984
6. Парфенова Л.Б., Вахрушев Д.С., Липовская Н.И. рынок услуг по обеспечению кибербезопасности как элемент инновационной инфраструктуры национальной экономической системы //Инновационное развитие экономики. — 2019. — № 5–1. — С. 54–59.
7. Три модели ИТ-аутсорсинга: что нам делать с парадигмой, 2016 / News.ru [Электронный ресурс] URL: https://alp-itsm.ru/info/articles/tri-modeli-it-outsorsinga-chto-nam-delat-s-paradigmoy/202016
8. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». URL: http://www.kremlin.ru/acts/bank/41460
9. Шилов С. Модели управления компанией / Архив журнала «Управление компанией», — №24 — 2013.
10. Янковская Е.С. Трансформация системы управления бизнесом в Российской Федерации в условиях глобальной цифровизации //Путеводитель предпринимателя. — 2020. — Т. 13. — № 2. — С. 37–45.
11. PwC /Technology Safety Board Information Security, 2020 report [Электронный ресурс] URL: https://www.pwc.com/gx/en/issues/cybersecurity/power-sector-cybersecurity.pdf
12. PwC Cyber Security M&A review. November, 2011[Электронный ресурс] URL: https://www.pwc.com/gx/en/aerospace-defence/pdf/cyber-security-mergers-acquisitions.pdf

Журнал «Современная наука: актуальные проблемы теории и практики»