Стратегии развития предприятий в условиях цифровизации

Игорь Александрович Вагнер
Магистр
Российский биотехнологический университет
Москва, Россия
vagner-1998@internet.ru
ORCID 0000-0000-0000-0000

Поступила в редакцию 01.02.2023
Принята 21.03.2023
Опубликована 15.04.2024

УДК 65.014.1:004
EDN LCOSTS
ВАК 5.2.3. Региональная и отраслевая экономика (экономические науки)
OECD 05.02.GY ECONOMICS

Аннотация

В статье рассматриваются вариации стратегии развития предприятий в условиях цифровизации. Обосновывается необходимость активного использования возможностей цифровизации для планирования и реализации стратегии развития. Анализируются наиболее перспективные и выгодные в экономическом плане, а также наиболее эффективные вектора использования цифровизации для стратегии прогрессивного развития. В условиях стремительного развития цифровых технологий предприятия сталкиваются с необходимостью адаптации и внедрения новых стратегий для обеспечения своей конкурентоспособности. В статье рассматриваются ключевые аспекты цифровизации бизнеса и ее влияние на стратегическое развитие предприятий. Анализируются современные тенденции и технологии, такие как искусственный интеллект, интернет вещей, блокчейн и большие данные, которые играют ключевую роль в трансформации бизнес-процессов. Особое внимание уделяется разработке цифровых стратегий, включающих изменение организационной структуры, развитие цифровой культуры и повышение квалификации сотрудников. Обсуждаются примеры успешных кейсов внедрения цифровых технологий в различных отраслях, а также выявляются основные вызовы и риски, связанные с цифровизацией. В заключение предлагаются рекомендации по эффективному управлению цифровыми преобразованиями, направленные на повышение эффективности и устойчивости предприятий в условиях быстро меняющейся цифровой среды.

Ключевые слова

стратегия развития, цифровизация, CRM-системы.

Введение

Стратегии развития предприятий в условиях цифровизации получили высокую степень актуальности за счёт акцентов на неизменный спутник стратегии развития в бизнесе – конкурентную разведку. И руководство любой компании, выстраивая стратегию развития, полностью осознает, что в информационно зависимом обществе своевременное получение информации и ее анализ – одно из основных преимуществ перед конкурентами (Ансофф, 2021).

Руководитель должен понимать, что и о его фирме, скорее всего, тоже собирают сведения, а потому защищать информацию о своем бизнесе не менее важно, чем уметь узнавать о чужом.

Коммерческая информация и ее защита являются важнейшей составляющей работы практически каждой компании. Организация планирования стратегии и ее развитие, пожалуй, любого вида бизнеса – это прежде всего борьба. Сначала борьба за то, чтобы войти на рынок, затем – чтобы

удержаться, закрепиться и расти. И практически всегда бизнес подвергается испытаниям на прочность в довольно агрессивной конкурентной среде. А это уже прямая ответственность коммерческого директора и главы отдела продаж.

Однако наверняка ни у кого нет желания становиться параноиком, маниакально запрещая любые попытки использовать общие базы. Поэтому первое, что предстоит проделать, это выделить зоны, конкретные точки, которые требуют защиты и в которых потеря или передача данных другим лицам (например, конкурентам) грозит бизнесу серьезными убытками.

Возможно, не совсем уместный пример, но в футболе при штрафном ударе игроки, стоящие в стенке, имеют шанс получить удар мячом в любую часть тела, но защищают они не ноги и не голову, а только то, что в данных обстоятельствах действительно оказывается самым уязвимым. Какое звено в коммерческом департаменте наиболее уязвимо? Клиентская база? Безусловно. Новации в продвижении, маркетинге, рекламе? Наверняка. Возможно, и в системе обучения менеджеров есть особые технологии, которыми не хочется делиться с конкурентами. В защите каждого из этих блоков большое значение имеют как методы организации контроля персонала и ограничения доступа к информации, так и программные, технические средства защиты.

Материалы и методы исследования

Определив болевые точки, нужно разработать такие методы защиты, которые бы съедали не более 20% потенциального бюджета компании и защищали ее как минимум на 80% – по закону Парето (Анцупов, 2020). Именно поэтому сегодня эффективная защита клиентских баз данных, документации и всего того, что является конкурентным преимуществом компании, невозможна без применения современных IT-технологий. Компании создают серьезные системы информационной безопасности не только по собственной инициативе, но и по требованию закона и отраслевых стандартов (ФЗ № 152 «О защите персональных данных» и стандарт PCI DSS для финансовых организации и банков). В связи с этим нужно учитывать сертификацию средств защиты в соответствии с требованиями законодательства и отраслевых стандартов.

Комплексные DLP-системы российских разработчиков укладываются в 3-4 млн рублей на парк из 250 компьютеров. Сюда же следует прибавить при необходимости стоимость оборудования (серверы, системы хранения данных и т.д.) и стоимость лицензий на программное обеспечение (ОС, СУБД и т.д.). В данном случае выбор и стоимость конкретной DLP-системы зависит от множества факторов – стоимости охраняемой информации, модели угроз и модели нарушителя, онлайн- или офлайн-режимов работы DLP-системы, возможных каналов утечки и т.д.). IT-методы защиты информации базируются на применении специальных программных систем, но даже в самом простом варианте для средней компании можно обойтись организационными мерами и простыми программными средствами и уложиться в 20-30 тыс. рублей, однако и уровень защиты будет соответствующий.

Отметим также, что с ростом требований растет и стоимость защиты, и здесь очень важно найти баланс между ее стоимостью, стоимостью защищаемой информации и удобством работы. При этом стоит помнить и о самом слабом звене – человеке, но в любом случае никакая система не обеспечит 100-процентной защиты. И здесь одну из значимых ролей играет повышение осведомленности людей в области информационной безопасности.

Результаты и обсуждение

Развитие и повсеместное использование компьютерных технологий приводит к тому, что защищать хранящуюся и обрабатываемую в информационных компьютерных системах информацию необходимо от большого количества угроз. Примеров из мировой практики, когда в целях конкурентной разведки или компрометации компании используются компьютерные технологии, более чем достаточно, вспомним хотя бы инцидент в банке HSBC. Уволенный сотрудник банка похитил реквизиты 15 000 клиентов. Пострадали пользовательские счета системы онлайн-банкинга, преимущественно жителей Швейцарии и Франции, в итоге банк сменил систему безопасности, что обошлось ему в 94 млн долларов.

Один из наиболее доступных способов защиты данных – разделение прав доступа к информации, обрабатываемой в виртуальной инфраструктуре, между IT-администратором и администратором службы безопасности. Стоит учитывать и то, что при возникновении угрозы информационной безопасности не всегда можно найти виновного. Часто виновным в утечке признается системный администратор, который по долгу службы раздавал права доступа пользователям. Поэтому правильно сделать так, чтобы сотрудники получали доступ к информации с ведома службы информационной безопасности.

Разумеется, внедрением DLP-систем работа по защите информации далеко не ограничивается. IT-технологии – это только часть, отдельный элемент, к которому предстоит еще прийти, создавая систему комплексной безопасности и защиты информации. Впрочем, сами по себе документы не являются гарантией абсолютного благополучия в плане информационной безопасности.

Так, в практике аудита стратегии развития нередко встречаются компании, у которых было все: и тщательно прописанные регламенты, и умные IT-специалисты с суперсовременными программами по защите информации, а утечки продолжались. В таком случае стоит обратить внимание на человеческий фактор, точнее, на то, как руководство компании организует и контролирует выполнение процедур по защите информации и как сотрудники выполняют эти процедуры.

Можем констатировать предварительные выводы: стратегии развития предприятий в условиях цифровизации базируются на аудите информационной безопасности предприятия, что представляют высокую степень актуальности и постоянно развиваются. Отсюда понимание, что стратегии развития предприятий в условиях цифровизации – это прежде всего безопасность, планирование с учетом рисков. Обоснуем эти утверждения (Ансофф, 2021):

Число инцидентов в области кибербезопасности постоянно растет, и единственный способ избежать серьезных проблем – выполнять регулярный аудит информационных ресурсов стратегии развития. Ни одна организация в мире не может выявить и устранить абсолютно все угрозы информационной безопасности. Но чем лучше определены слабые места в стратегии развития компании, тем проще сотрудникам отдела IT-безопасности сосредоточить на них свое внимание и разработать план снижения рисков, чтобы защитить ценные данные, навести порядок в файловых хранилищах и предоставить сотрудникам лишь необходимый доступ к данным стратегии развития. Для этого можно применить следующие меры:

– определить все IT-активы стратегии развития, потеря или раскрытие которых нанесет ущерб бизнесу;
– проанализировать бизнес-процессы стратегии развития, которые зависят от IT-активов;
– продумать, какие именно события могут повлиять на эти активы и насколько они вероятны;
– сформулировать угрозы, которые нужно устранить для смягчения рисков;
– разработать новый план снижения рисков или скорректировать старый в регламентах стратегии развития.

Аудит рисков информационных ресурсов стратегии развития можно выполнить самостоятельно с помощью штатных инструментов Windows, но лучше использовать автоматизированные средства, которые проанализируют слабые места и усилят кибербезопасность современными методами. Оценка рисков информационных ресурсов стратегии развития требует затрат, но экономить точно не стоит, и вот почему. Узнать профиль риска – значит, найти слабые места стратегии развития. Например, определить источники внутренних угроз:

– взять на контроль цифровой след уволенных сотрудников с сохраненным доступом к ресурсам компании;
– определить характер риска:
– установить контроль за доступом к коммерческой тайне и т.д.;
– рассчитать вероятность наступления инцидента (Чернышев, 2019);
– проранжировать риски стратегии развития от наиболее вероятных к менее, особое внимание уделив первым;

– выявить и устранить уязвимости.

В этой связи отметим, что методология оценки рисков стратегии развития помогает не только найти уязвимости, но и понять, как их устранить. Тот, кто проводит аудит, ставит себя на место злоумышленника: какая информация стратегии развития представляет интерес, какую выгоду можно из нее извлечь? Благодаря такому подходу можно сравнить желаемый уровень безопасности стратегии развития с реальным и определить шаги к достижению более высокого уровня.

Иногда, чтобы проверить надежность средств безопасности и протоколов, приглашают специалиста с навыками хакера. Профессионал способен закрыть информацию для посторонних, убрать секретные документы стратегии развития из общего доступа, убедиться, что конфиденциальные бумаги стратегии развития не копируют, а также провести инвентаризацию информационных активов стратегии развития. Ведь далеко не каждый руководитель бизнеса представляет себе объем всех IT-активов стратегии развития, а такая оценка риска кибер-угроз помогает разобраться в структуре ценной для компании информации. Для ясности разберем ситуацию с выбором компанией целевого рынка, для чего определим целевые рынки смоделированного социального предприятия. К таким компаниям, как правило, относятся те, которые:

– принимают на работу социально уязвимые категории граждан, например, инвалидов, многодетных родителей, пред пенсионеров. Они должны составлять четверть от общего количества персонала;

– производят товары или оказывают услуги для социально незащищенных граждан. Доля дохода в общем объеме должна быть не менее 50%;

– обеспечивают доступ работ, товаров, услуг, произведенных социально незащищенной категорией граждан, к рынкам сбыта;

– оказывают услуги в сфере реабилитации и уходу на дому, в сфере дополнительного образования, отдыха инвалидов, детей, пенсионеров.

К примеру, компания «Весна» выпускает телевизоры с разрешением 8К и вогнутым экраном. Четверть персонала относится к социально уязвимым категориям граждан. На рынке представлено огромное количество аналогичного товара. За каждого клиента идет острая конкурентная борьба. И в данном случае лояльные клиенты всегда выгодны для компании по следующим причинам:

– снижаются затраты, необходимые на привлечение, удержание;

– они всегда менее восприимчивы к завышенной цене, так как довольны продукцией;

– готовы порекомендовать продукцию своим знакомым;

– защищают репутацию компании при наличии негативных отзывов.

Выбор целевого рынка в рассматриваемом примере происходит по трем направлениям:

– сегментации по продукту;

– сегментации по преимуществам продукта;

– сегментации по потребностям клиентов.

Плюс учитывается сегментация рынка. Таким способом определяют свой рынок, который будет автоматически влиять на лояльность потенциальных клиентов. При сегментации рынка выявляют группы потребителей с близкими потребностями, похожим покупательским поведением и основными характеристиками.

Если компания работает на рынке B2C, учитывают:

– географические критерии, то есть территорию, с которой компания планирует работать (страну, город, регион);

– социально-демографические критерии (социальный статус, возраст, образование, пол, уровень дохода и т. д.);

– поведенческие критерии (ценности, потребности, образ жизни, критерии выбора и использования).

При работе компании на рынке B2B учитывают тот же набор критериев.

Как осуществляется выбор целевого международного рынка? Этот вариант рассмотрим на примере указанной компании «Весна».

В международной сегментации компания принимала во внимание следующее:

– ограниченное число клиентов и объема значительных контрактов;
– производные спроса и низкой эластичности спроса;
– тесные связи между поставщиками и производителем;
– географическую концентрацию.

Важно учитывать, что международный рынок перенасыщен товарами. Поэтому привлечь потенциальных клиентов можно только выгодными условиями сотрудничества, доступными ценами и дополнительными бонусами. Информационные активы стратегии развития – это важные для бизнеса данные на любом носителе.

IT-активы стратегии развития бывают (Бархоленко, 2022):

– открытыми — можно распространить без ущерба;
– для служебного пользования – огласка спровоцирует репутационные и финансовые риски;
– конфиденциальными – с ограниченным доступом или с грифом «Секретно». Доступны только нескольким людям из топ-менеджмента.

Утечка нанесет непоправимый вред компании.

Заключение

Без понимания того, что нужно защищать, в каком объеме и где эта информация находится, дальнейшие шаги в области безопасности бессмысленны. А снизить расходы можно благодаря следующим мерам:

– провести точную оценку IT-активов стратегии развития и их защищенности. Проследить, куда именно направить ресурсы, чтобы снизить риски. Это дешевле, чем постоянно сканировать все участки IT-контура стратегии развития и активно защищать те, где риски минимальны;
– проконтролировать исполнение требований закона. Беречь информацию стратегии развития от утечки важно не только в интересах компании. Этого требует законодательство. В числе таких документов – Закон №152-ФЗ «О персональных данных», Требования ФСТЭК по обеспечению мер безопасности для объектов КИИ, Стандарт по обеспечению информационной безопасности банков РФ СТО БР ИББС.

В случае если компания в своей стратегии развития вышла на международный уровень, она обязана подчиняться и требованиям международного законодательства в области раскрытия данных,

проводить оценку по GDPR и соблюдать стандарты PCI DSS или SOX при работе с контрагентами из ЕС.

Также отраслевая специфика накладывает дополнительные обязательства: например, медицинские организации обязаны соблюдать HIPAA, который обеспечивает сохранность баз данных пациентов.

Подытожив все вышесказанное, можно сделать вывод о том, что утечки финансовых отчетов, информации о новом продукте, персональных данных сотрудников и клиентской базы опасны для компании. В этом случае компании придется платить штрафы, уступать конкурентам, отчитываться перед Роскомнадзором, отрабатывать негатив в СМИ и т.д.

В любых ситуациях самым надежным способом профилактики неприятностей стратегии развития будет регулярно проводить аудит рисков. Это не просто сохранит компании критически важные данные, но и поможет в создании эффективной политики безопасности, наладит взаимопонимание между руководством компании, IT-отделом и офицерами безопасности. Важно реализовать четкую программу кибербезопасности, которая сэкономит деньги и защитит от ненужного внимания Роскомнадзора и негатива в СМИ.

Таким образом мы связали цифровую безопасность и вектор стратегии развития предприятий в условиях цифровизации.

Список литературы

1. Ансофф И. Новая корпоративная стратегия. СПб.: Питер, 2021. 416 с.
2. Анцупов Ф.Я. Стратегическое управление: моногр. 4-е перераб. изд. М.: Проспект, 2020. 344 с.
3. Бархоленко В.А. Механизмы страхования в управлении рисками информационной безопасности // Экономический анализ: теория и практика. 2022. № 2. С. 379-388.
4. Бурыкин А.Д., Костоева Е.Х. Организация риск-менеджмента на предприятии // Вестник научных конференций. 2020. № 4. С. 29-31.
5. Васильева Е.Е. Актуальные проблемы риск-менеджмента в России // Инновационная наука. 2021. № 6. С. 54 - 56.
6. Власов А.В. Управление организацией в информационном обществе: поведенческий риск-менеджмент // Модели, системы, сети в экономике, технике, природе и обществе. 2020. № 3. С. 22-31.
7. Гибсон Дж., Иванцевич Д.М., Доннелли Д.Х. Организации: поведение, структура, процессы: пер. с англ. М.: ИНФРА-М, 2020. 415 с.
8. Голубева С.С., Рзаева Л.Р. Особенности формирования системы риск-менеджмента предприятия // Бизнес и стратегии. 2020. № 3. С. 26-30.
9. Остервальдер А., Пинье И. Построение бизнес-моделей: Настольная книга стратега и новатора. Пер. с англ. М.: Альпина Паблишер, 2019. 288 с.
10. Петросова В.В. Проблемы финансового риск-менеджмента в России и способы повышения его эффективности // Символ науки. 2020. № 1. С. 204-207.
11. Чернышев М.А. Стратегический менеджмент. Основы стратегического управления. Ростов н/Д: Феникс, 2019. 506 с.

Strategies for the development of enterprises in the context of digitalization

Igor A. Wagner
Master
Russian University of Biotechnology
Moscow, Russia
vagner-1998@internet.ru
ORCID 0000-0000-0000-0000

Received 01.02.2023
Accepted 21.03.2023
Published 15.04.2024

UDC 65.014.1:004
EDN LCOSTS
VAK 5.2.3. Regional and sectoral economics (economic sciences)
OECD 05.02.GY ECONOMICS

Abstract

The article discusses variations in enterprise development strategies in the context of digitalization. It justifies the need for active use of digitalization opportunities for planning and implementing development strategies. The most promising and economically advantageous, as well as the most effective vectors of digitalization use for progressive development strategies, are analyzed. In the context of rapid digital technology development, enterprises face the need to adapt and implement new strategies to ensure their competitiveness. The article examines key aspects of business digitalization and its impact on the strategic development of

enterprises. Modern trends and technologies such as artificial intelligence, the Internet of Things, blockchain, and big data, which play a key role in transforming business processes, are analyzed. Special attention is given to the development of digital strategies, including changes in organizational structure, the development of digital culture, and employee upskilling. Examples of successful cases of digital technology implementation in various industries are discussed, as well as the main challenges and risks associated with digitalization. In conclusion, recommendations for effective management of digital transformations are proposed, aimed at increasing the efficiency and sustainability of enterprises in a rapidly changing digital environment.

Keywords
development strategy, digitalization, CRM systems.

References

1. Ansoff I. New corporate strategy. St. Petersburg: St. Petersburg, 2021. 416 p.
2. Antsupov F.Ya. Strategic management: monograph. 4th edition. Moscow: Prospect, 2020. 344 p.
3. Barkholenko V.A. Insurance mechanisms in information security risk management // Economic analysis: theory and practice. 2022. № 2. pp. 379-388.
4. Burykin A.D., Kostoeva E.H. Organization of risk management at the enterprise // Bulletin of scientific conferences. 2020. № 4. pp. 29-31.
5. Vasilyeva E.E. Actual problems of risk management in Russia // Innovative science. 2021. № 6. pp. 54-56.
6. Vlasov A.V. Organization management in the information society: behavioral risk management // Models, systems, and networks in economics, technology, nature, and society. 2020. № 3. pp. 22-31.
7. Gibson J., Ivantsevich D.M., Donnelly D.H. Organizations: behavior, structure, processes: trans. from English M.: INFRA-M, 2020. 415 p.
8. Golubeva S.S., Rzaeva L.R. Features of the formation of the enterprise risk management system // Business and strategies. 2020. № 3. pp. 26-30.
9. Osterwalder A., Pinye I. Building business models: A strategist and innovator's Handbook. Translated from English M.: Alpina Publisher, 2019. 288 p.
10. Petrosova V.V. Problems of financial risk management in Russia and ways to improve its effectiveness // A symbol of science. 2020. № 1. pp. 204-207.
11. Chernyshev M.A. Strategic management. Fundamentals of strategic management. Rostov n/A: Phoenix, 2019. 506 p.