УДК 338

ПРОБЛЕМЫ БЕЗОПАСНОСТИ И КИБЕРБЕЗОПАСНОСТИ, КАК ПЕРСПЕКТИВНЫЕ РЫНКИ. СТРАТЕГИИ РАЗВИТИЯ

В. С. Аржевикина, М. А. Аксенов
Научный руководитель: О. В. Гостева, к. э. н., доцент

ФГБОУ ВО «Сибирский государственный университет науки и технологии им. ак. М. Ф. Решетнева»
Российская Федерация, 660037, г. Красноярск, просп. Имени газеты «Красноярский рабочий», 31
valeria.arzhevikina@yandex.ru

В данной статье рассматриваются проблемы безопасности и кибербезопасности на 2023 г., изучены рынки кибербезопасности ведущих стран мира, а также представлены стратегии развития как для этих рынков, так и для развития кибербезопасности в целом.

Ключевые слова: кибербезопасность, рынки кибербезопасности, стратегии развития.

SECURITY AND CYBERSECURITY ISSUES AS PROMISING MARKETS. DEVELOPMENT STRATEGIES

V. S. Arzhevikina, M. A. Aksenov
Supervisor: O. V. Gosteva, Candidate of Economic Sciences, Associate Professor

Reshetnev Siberian State University of Science and Technology
31, Krasnoyarsky Rabochy Av., Krasnoyarsk, 660037, Russian Federation
valeria.arzhevikina@yandex.ru

This article examines the problems of security and cybersecurity for 2023, examines the cybersecurity markets of the leading countries of the world, and presents development strategies for both these markets and for the development of cybersecurity in general.

Keywords: cybersecurity, cybersecurity markets, development strategies.

В современном мире безопасность стала одной из наиболее важных областей каждой сферы жизни. Безопасность информации и защита от киберугроз стали ключевыми задачами для организаций и частных лиц. Это открыло перспективные возможности развития на рынке безопасности и кибербезопасности.

Рынок безопасности охватывает широкий спектр сегментов, таких как физическая безопасность (охрана объектов и территорий), инфраструктурная безопасность (энергетика, транспорт, коммуникации), корпоративная безопасность (защита бизнес-процессов, информационные системы) и даже личная безопасность (домашняя и персональная безопасность).

Особое внимание сегодня уделяется кибербезопасности. С ростом Интернета и развитием цифровых технологий киберугрозы становятся все более серьезной проблемой. Киберпреступники постоянно ищут новые способы атак на системы и данных, и поэтому рынок кибербезопасности растет стремительными темпами.

Стратегия развития рынка безопасности и кибербезопасности включает несколько ключевых моментов:

Расширение предложения. Развитие новых технологий, таких как искусственный интеллект, машинное обучение и блокчейн, позволяет создавать более эффективные системы защиты. Развитие таких продуктов и услуг будет способствовать росту рынка.

Повышение осведомленности. Образование и повышение осведомленности пользователей и организаций о кибербезопасности играют ключевую роль в борьбе с киберугрозами. Расширение программ обучения и информационных кампаний поможет укрепить безопасность в цифровом мире.

Глобальное сотрудничество. Киберугрозы не ограничиваются границами стран, поэтому глобальное сотрудничество между правительствами, организациями и компаниями является необходимостью.

Обмен информацией, координация усилий и разработка международных стандартов помогут повысить безопасность в целом.

В свете все более частых киберугроз и угроз для безопасности, рынок безопасности и кибербезопасности представляет огромные возможности для инноваций и бизнеса.

Стратегия развития, которая включает расширение предложения, повышение осведомленности и глобальное сотрудничество, поможет укрепить уровень защиты и создать успешные предприятия в этой области.

Рынок безопасности включает в себя широкий спектр продуктов, услуг и решений, которые направлены на обеспечение безопасности в различных сферах деятельности. Это может быть, как физическая (охрана объектов, видеонаблюдение), так и корпоративная безопасность (защита информации и бизнес-процессов), а также личная безопасность (домашняя безопасность, охрана личных данных).

Кибербезопасность – это сегмент рынка безопасности, который специализируется на защите от киберугроз. В современном цифровом мире, где все больше информации и бизнес-процессов осуществляется онлайн, кибербезопасность становится критически важной. Киберугрозы включают в себя хакерские атаки, вирусы, фишинг, кибершпионаж и другие виды мошенничества в сети.

Кибербезопасность является одним из самых быстрорастущих сегментов рынка безопасности. Это обусловлено не только цифровой трансформацией и увеличением числа устройств, подключенных к Интернету (интернет вещей), но и постоянно развивающимися методами кибератак и появлением новых видов угроз.

Участники рынка безопасности и кибербезопасности включают в себя различные организации и компании:

Поставщики технологий и продуктов. Это предприятия, которые разрабатывают и поставляют инновационные технологии и продукты в области безопасности и кибербезопасности. Это могут быть антивирусные программы, системы мониторинга, бренды сетевой безопасности и другие решения.

Консультационные и аудиторские компании. Эти организации предоставляют консультационные услуги в области безопасности, помогают компаниям анализировать свои уязвимости и разрабатывать стратегии защиты.

Компании по обучению и сертификации. Такие организации предлагают обучение и сертификацию специалистов в области безопасности и кибербезопасности. Они помогают профессионалам развивать свои навыки и повышать квалификацию.

Государственные органы и правительства. Государственные учреждения занимаются разработкой и внедрением законодательства в области кибербезопасности, а также контролируют выполнение соответствующих норм и правил.

Рынки безопасности и кибербезопасности имеют огромный потенциал роста в будущем. Повышение осведомленности о киберугрозах, строгие требования по обеспечению безопасности, а также постоянное развитие новых технологий и решений будут продолжать стимулировать рост этих рынков.

Рынок кибербезопасности в США является одним из самых крупных и динамично развивающихся. Вот некоторые ключевые аспекты и характеристики этого рынка:

Расширение инвестиций.ю США активно инвестируют в кибербезопасность как государство, так и частные компании. Имеется значительный спрос на инновационные решения

и технологии в области кибербезопасности, что создает благоприятные условия для развития рынка.

Развитие киберугроз. США являются одной из наиболее целевых стран для кибератак со стороны злоумышленников. Это создает повышенный спрос на решения и услуги по защите информации и борьбе с киберугрозами.

Государственная поддержка. Правительство США активно внедряет меры по обеспечению кибербезопасности и поощряет сотрудничество между государственными органами, частным сектором и исследовательскими учреждениями. Это способствует развитию инновационных решений и стимулирует рост рынка.

Нормативные требования. США имеют строгие нормативные требования в области кибербезопасности, особенно в секторах финансов, здравоохранения и критической инфраструктуры. Это создает растущий рынок для компаний, предлагающих соответствующие решения и услуги.

Киберзащитные компании. В США базируется значительное количество киберзащитных компаний, которые разрабатывают инновационные продукты и услуги в области кибербезопасности. Это способствует конкуренции и стимулирует рост рынка.

Партнерство с правительством. Многие компании по кибербезопасности в США устанавливают партнерские отношения с правительственными организациями для предоставления услуг и разработки общих стратегий по борьбе с киберугрозами.

Рынок кибербезопасности в США предоставляет широкий спектр возможностей для компаний в области разработки технологий безопасности, услуг по кибербезопасности и консалтинговых услуг. При условии активного внедрения инновационных решений и соблюдения высоких стандартов безопасности, это перспективный и конкурентоспособный рынок для бизнеса.

Рынки кибербезопасности России стремительно развиваются! Существует растущий спрос на продукты и услуги, направленные на защиту от киберугроз. Множество компаний предлагают решения, включающие антивирусные программы, файерволы, системы мониторинга и обнаружения инцидентов, а также профессиональные услуги по аудиту и консультациям в области кибербезопасности.

В России также созданы специальные центры и инкубаторы по кибербезопасности, способствующие поддержке и развитию стартапов в этой области. Онлайн-безопасность стала важной темой для правительства, организаций и обычных пользователей.

Однако, как и везде, рынок кибербезопасности также стал объектом интереса для киберпреступников. Поэтому важным фактором в развитии этой отрасли является постоянное обновление и совершенствование методов защиты, а также повышение осведомленности пользователей о киберугрозах.

В целом, российские рынки кибербезопасности продолжают расти и развиваться, стремясь обеспечить безопасность в цифровом пространстве.

Проблемы безопасности и кибербезопасности являются перспективными рынками, требующими постоянного развития и инноваций. Несколько стратегий, которые могут способствовать развитию этих рынков:

Исследование и разработка. Увеличение инвестиций в исследования и разработку новых технологий и методов безопасности станет ключевым фактором. Новые угрозы появляются каждый день, поэтому необходимо постоянно заниматься разработкой инновационных решений.

Сотрудничество и партнерство. Установление партнерских отношений с другими компаниями и организациями в сфере безопасности может усилить мощности и расширить сферу влияния на рынке. Совместные исследования и обмен опытом могут способствовать развитию лучших практик и инноваций.

Образование и осведомленность. Создание программ образования и повышения осведомленности о кибербезопасности поможет подготовить кадры, способных бороться с угрозами и развиваться в этой области.

Регулирование и законодательство. Разработка и соблюдение соответствующих законов и нормативов в области кибербезопасности является важным аспектом защиты информации и создания доверия у клиентов.

Сегментирование рынка. Определение конкретных сегментов рынка и предложение специализированных решений для каждого сегмента поможет более точно удовлетворять потребности клиентов и получать конкурентные преимущества.

Глобальное присутствие. Расширение деятельности и налаживание партнерств за пределами родной страны позволит достичь мирового признания и привлечь новых клиентов.

Эти стратегии могут помочь компаниям в области безопасности и кибербезопасности развиваться, приспосабливаться к изменяющимся условиям и оставаться конкурентоспособными на перспективных рынках.

Список использованных источников

1. Современные технологии: их виды и применение в современном мире [Электронный ресурс] // Базы удачи. – Режим доступа: https://baziudachi.ru/faq/sovremennye-te. – Дата доступа: 17.10.2023.

2. Об угрозах [Электронный ресурс] // Kaspersky. – Режим доступа: https://www.kaspersky.ru/resource-center. – Дата доступа: 18.10.2023.

3. Справочник – лекции, шпаргалки, теория и практика [Электронный ресурс] // Научные Статьи. Ру. — Режим доступа: https://NauchnieStati.ru/spravka/profess... – Дата доступа: 18.10.2023.

4. Принцип обеспечения безопасности [Электронный ресурс] // Zvenst/ru. – Режим доступа: https://zvenst.ru/principy-obespeceniya-bezopasnosti/. – Дата доступа: 18.10.2023.

5. Защита от угрозы цифрового мира: что такое кибербезопасность и кто ей занимается [Электронный ресурс] // Практикум яндекс. – Режим доступа:https://practicum.yandex.ru/blog/-chto-takoekiberbrzopasnost/. – Дата доступа: 18.10.2023.

6. Важность безопасности в современном мире [Электронный ресурс] // Новые гайды каждый день. – Режим доступа: https://pro-zamenu.ru/posty/1-sentyabrya-2023-goda-vazhnost-bezopasnosti-v-sovremennom-mire.html. – Дата доступа: 18.10.2023.

References

1. "Modern technologies: both types and applications in the modern world" [Electronic resource] //Databases: [website]. — URL: https://baziudachi.ru/faq/sovremennye-te (date of application: 17.10.2023)

2. "About the threat" [Electronic resource] // Kaspersky: [website]. — URL: https://www.kaspersky.ru/resource-center (accessed: 10/18/2023)

3. "Specialist- lecture, pargalki, theory and practice" [Electronic resource] //Scientific articles. <url>: [website]. — URL: https://NauchnieStati.ru/spravka/profess ... (accessed: 10/18/2023)

4. "Example of a security description" [Electronic resource] // Zvenst/ru: [website]. — URL: https://zvenst.ru/principy-obespeceniya-bezopasnosti / (accessed: 10/18/2023)

5. "Zenith from the amazing world: what is cybersecurity and who understands it" [Electronic resource] //Yandex Workshop: [website]. — URL:https://практикум .<url>/blog/what is cybersecurity/ (publication date: 18.10.2023)

6. "The importance of security in the modern world" [Electronic resource] //New guides every day [website]. — URL: https://pro-zamenu.ru/posty/1-sentyabrya-2023-goda-vazhnost-bezopasnosti-v-sovremennm-mire.html (accessed: 10/18/2023)