11. Отчет о воздействии за 2021 год // Сбербанк URL: https://www.sberbank.com/common/img/uploaded/files/pdf/normative_docs/sber_impact_report_for_2021_ru.pdf(дата обращения: 16.11.2023)

Шао Линь дзянь,
магистрант
Сапун О.Л.,
к.пед.н., доцент
БГАТУ
г. Минск, Беларусь

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КИТАЯ

Аннотация: В статье рассматривается информационная безопасность Китая и возможности в области кибербезопасности для усиления защиты личной информации в цифровой экономике. Приведены популярные и передовые компании в области кибербезопасности Китая.

Ключевые слова: кибербезопасность; информационная безопасность; защита информации; сетевая безопасность

Эволюция кибербезопасности открывает многочисленные возможности для бизнеса и организаций. В последние годы Китай расширил свои возможности в области кибербезопасности из-за опасений по поводу безопасности своих национальных данных и необходимости усиления защиты личной информации в цифровой экономике.

В 2021 году масштаб китайского рынка кибербезопасности достиг 62,7 млрд юаней (8,64 млрд долларов США), увеличившись на 9,5 млрд юаней (1,3 млрд долларов США), или 17 процентов, по сравнению с 2020 годом. Рынок кибербезопасности страны вступил в период быстрое развитие, в основном обусловленное двумя факторами: соблюдением политики и модернизацией промышленности. Услуги сетевой безопасности стали самым быстрорастущим направлением на рынке, поскольку предприятия выделяют более высокий бюджет своих расходов на безопасность на услуги кибербезопасности.

В 2022 году выручка китайского рынка кибербезопасности достигает 14,05 млрд долларов США. В результате ожидается, что к 2027 году китайский рынок кибербезопасности будет расти со среднегодовыми темпами роста (CAGR) примерно на 12,4 процента [1] (Рис. 1)

В эпоху цифровых технологий китайские компании несут ответственность за постоянно растущее количество транзакций информации и данных. Эти предприятия в настоящее время являются основными

объектами кибератак, и из-за проблем организационных систем часто происходят утечки информации.

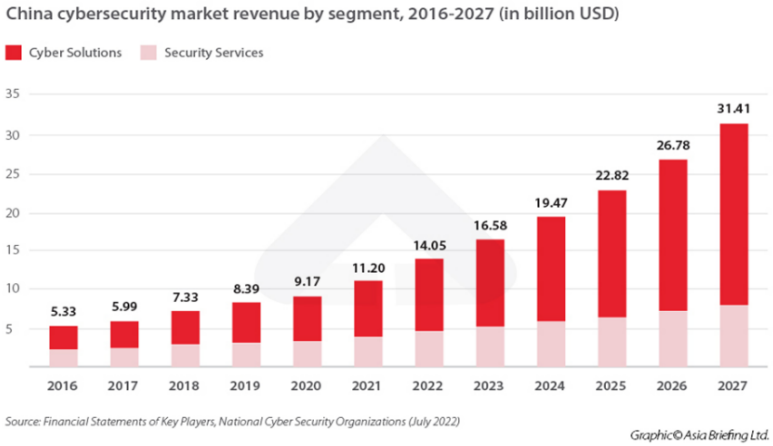

Рис. 1. Рост выручки китайского рынка кибербезопасности 2016-2027 гг.

Другим фактором являются темпы расширения покрытия и скорости Интернета. Примером этого является проект Broad band China Project, целью которого является предоставление доступа к контролируемым высокоскоростным широкополосным сетям 95 процентам городского населения. Кроме того, Государственный совет Китая планирует инвестировать 22 миллиарда долларов США в расширение инфраструктуры широкополосной сети в сельских районах страны. Эти инвестиции направлены на предоставление улучшенных интернет-услуг примерно 30 миллионам домохозяйств и охватывают около 50 000 деревень.

В Китае большое количество пользователей смартфонов. В этих смартфонах используются различные приложения, собирающие конфиденциальные персональные данные. Приложения для обработки онлайн-транзакций и социальные сети делают Интернет очень уязвимым местом, подвергающим данные пользователей кибератакам.

Инструменты кибербезопасности необходимы для управления и защиты индивидуальных и корпоративных угроз в Интернете, тем самым стимулируя спрос на продукты кибербезопасности в Китае.

Предприятия осознают преимущества экономии денег и ресурсов за счет перемещения своих данных в облако, а не за счет создания и обслуживания новых хранилищ данных, что стимулирует спрос на облачные решения и последующий рост использования средств безопасности по требованию услуги.

Эти преимущества побуждают крупные корпорации, а также малые и средние предприятия в Китае чаще внедрять облачные решения. Прогнозируется, что в ближайшие годы облачные платформы и экосистемы послужат катализатором быстрого увеличения объема и масштабов цифровых инноваций.

В 2021 году порталом обмена информацией МИИТ об угрозах и уязвимостях информационной безопасности было задокументировано 143 319 уязвимостей информационных систем. 86 217 из них были отнесены к категории «среднего риска», а 40 498 — к «высокому риску».

В то же время компании China Telecom, China Mobile и China Unicom в 2021 году сообщили о 753 018 распределенных атаках типа «отказ в обслуживании» (DDoS), что на 43,9 процента меньше, чем в 2020 году. Количество угроз и уязвимостей кибербезопасности, о которых сообщалось по состоянию на 2021 год, их число составило 88 799, что на 60,9 процента меньше, чем за тот же период 2020 года [2].

В Китае резко возросло число инцидентов, связанных с кибербезопасностью, из-за растущего организационного внедрения цифровизации и использования связанных с ней технологий в рамках корпоративных операций. Благодаря сетям 5G китайские устройства теперь более взаимосвязаны, чем когда-либо.

Кроме того, уровень утечки личной информации среди пользователей Интернета был самым высоким - 22,1 процента; Интернет-мошенничество затронуло 16,6 процентов пользователей; 9,1 процента пользователей сообщили, что их устройства были заражены вирусами, а 6,6 процента из них сообщили, что их учетные записи или пароли были украдены.

Кибербезопасность в Китае быстро становится синонимом национальной безопасности и государственного суверенитета. Чтобы сократить разрыв с международными коллегами в США и ЕС и улучшить общую безопасность и обороноспособность страны, китайское правительство приняло ряд нормативных мер, направленных на усиление сетевой безопасности.

Трехлетний план кибербезопасности Пекина одновременно является стратегией киберзащиты, направленной на укрепление своих цифровых активов в рамках стремления к созданию устойчивой цифровой экономики.

Национальный 14-й пятилетний план предлагает укрепить системы гарантий кибербезопасности и наращивание потенциала, ресурсы данных, а также сети и информационные системы в важнейших секторах.

Чтобы сосредоточиться на защите сетей и данных в Китае, правительство приняло первый в стране Закон о кибербезопасности в 2016 году, который вступил в силу в 2017 году. Чтобы привести закон в соответствие с различными законами, принятыми после него, было выпущено несколько поправок к Закону о кибербезопасности.

Ниже приведены некоторые из самых популярных и передовых компаний в области кибербезопасности со штаб-квартирой в Китае по данным Cybersecurity Ventures (2020)[3]:

AntiyLabs: базирующаяся в Пекине компания AntiyLabs является создателем антивирусного ядра нового поколения. Ведущий поставщик, предлагающий лучшее в своем классе антивирусное ядро и передовые антивирусные услуги для борьбы с вредоносным ПО для ПК и мобильных устройств, с шестью исследовательскими центрами.

Bangcle: ведущий поставщик услуг и решений по обеспечению безопасности Интернета вещей и мобильных приложений.

ZhizhangyiScience&TechnologyCo., Ltd: пекинская компания лидер рынка решений для обеспечения безопасности мобильных устройств для бизнеса. В настоящее время эта компания расширяет свою платформу ситуационной осведомленности о безопасности, чтобы обеспечить визуализацию больших данных и демонстрацию преимуществ продукта.

Bluedon: ключевой игрок на китайском рынке информационной безопасности, он предоставляет клиентам из различных отраслей универсальные решения по информационной безопасности благодаря своей бизнес-модели развития связей «четыре в одном», которая включает в себя продукты безопасности, решения безопасности, услуги и операции по обеспечению безопасности.

BUGBANK: является сторонником открытой безопасности и брендом сетевой безопасности, принадлежащим Shanghai Muler Network Technology Co., Ltd. Представляет винстументы для сбора, изучения, устранения и отслеживания самых последних уязвимостей Интернета, работает с международными специалистами по сетевой безопасности.

DBAPP Security, Ltd: пионер в области облачных вычислений, больших данных, умных городов, мобильного Интернета, безопасности веб-приложений и безопасности баз данных.

H3C: лидер рынка цифровых решений, стремящийся быть самым надежным партнером клиентов в области бизнес-инноваций и модернизации промышленности.

i-Sprint: ведущий поставщик средств идентификации и безопасности транзакций в цифровой сфере, который позволяет людям, предприятиям и сообществам развивать систему обеспечения посредством цифровой идентификации и идентификации вещей (IDoT).

QIANXIN: интегрированная компания, предлагающая государственному сектору и бизнесу товары безопасности нового поколения.

Threatbook: ведущий поставщик информации об угрозах безопасности в Китае. С момента своего основания в 2015 году ThreatBook защитил миллионы китайских компьютеров с помощью своих аналитических данных и сервисов.

ИТ-индустрия Китая находится на подъеме, и все больше и больше китайских компаний выходят на международный рынок. В результате индустрия кибербезопасности страны, которая является важной поддержкой китайской национальной стратегии в области безопасности, также вступает в критический период внедрения инновационных продуктов, технологий.

В настоящее время цепочка индустрии сетевой безопасности Китая постепенно улучшается, и есть предприятия, которые предоставляют как продукты, так и услуги. Более того, кибербезопасность в Китае постепенно становится приоритетом в новых сценариях применения, таких как облачные вычисления, промышленный Интернет и Интернет вещей (IoT).

Список литературы

1. China’s Cybersecurity Industry: A Market Analysis https://www.china-briefing.com/news/chinas-cybersecurity-industry-a-market-analysis/

2. Cybersecurity - China https://www.statista.com/outlook/tmo/ cybersecurity/china

3. China Cybersecurity Companies https://cybersecurityventures.com/china-cybersecurity-companies/