**МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY**

**DOI: https://doi.org/10.18454/itech.2024.2.2**

# АНАЛИЗ РЕШЕНИЙ ПО КИБЕРБЕЗОПАСНОСТИ В США НА ОСНОВЕ СТРАТЕГИИ ПРАВИТЕЛЬСТВА США

Научная статья

**Васильев А.[1, *]**
[1] ORCID : 0009-0008-9909-2385;
[1] ScienceSoft, Минск, Беларусь

* Корреспондирующий автор (alexey_vasilyev96[at]mail.ru)

**Аннотация**

Целью статьи является анализ продаж решений по кибербезопасности в США. Методы исследования заключаются в анализе статистических сборников и отчетов по кибер- и информационной безопасности. В статье приведен обзор рынка кибербезопасности США. Рассмотрены основные поставщики решений по кибербезопасности не только на рынкае США, но и на общемировом рынке в целом. Изучены показатели выручки от реализации решений по кибербезопасности отдельных компаний США. Даны прогнозы по развитию данной отрасли. Рассмотрены и изучены тенденции повышения спроса и расходов на решения по кибербезопасности, а также сопутствующие препятствия и риски для компаний по предоставлению услуг кибербезопасности. Определена роль правительства США в развитии кибербезопасности страны.

**Ключевые слова:** кибербезопасность, киберугрозы, продажи, выручка, стратегия кибербезопасности.

# AN ANALYSIS OF CYBERSECURITY SOLUTIONS IN THE U.S. BASED ON U.S. GOVERNMENT STRATEGY

Research article

**Vasilyev A.[1, *]**
[1] ORCID : 0009-0008-9909-2385;
[1] ScienceSoft, Minsk, Belarus

* Corresponding author (alexey_vasilyev96[at]mail.ru)

**Abstract**

The aim of the article is to analyse the sales of cybersecurity solutions in the United States. The research methods consist of analysing statistical compilations and reports on cyber and information security. The article provides an overview of the US cybersecurity market. The main suppliers of cybersecurity solutions not only in the US market, but also in the global market as a whole are examined. Revenue figures from the implementation of cybersecurity solutions by individual US companies have been investigated. Prognoses for the development of this industry are given. The tendencies of increasing demand and expenditures for cybersecurity solutions, as well as related obstacles and risks for cybersecurity services companies, are examined and analysed. The role of the U.S. government in the development of cybersecurity in the country is defined.

**Keywords:** cybersecurity, cyber threats, sales, revenue, cybersecurity strategy.

## Введение

В Соединенных Штатах Америки один из самых высоких в мире показателей проникновения цифровых технологий. Многие пользователи и организации активно используют устройства интернета вещей (IoT) и облачные решения. В своей повседневной деятельности организации по всей территории США все больше полагаются на компьютерные сети, интеллектуальные устройства и электронные данные, что, в свою очередь, приводит к увеличению объемов личной и финансовой информации, передаваемой и хранимой в Интернете. Следовательно, потребность в решениях для управления безопасностью, идентификацией и доступом к данным с каждым годом становится все более острой. И прежде, чем перейти к основной части наших исследований, определимся с основными понятиями и определениями, принятыми в США на уровне государства.

## Термины и определения

Стандарт ISO/IEC 27032:20121 [1]. ISO – международная независимая неправительственная организация, в состав которой входят 167 национальных органов по стандартизации (США является учредителем). Кибербезопасность (или безопасность киберпространства) определяется как сохранение конфиденциальности, целостности и доступности информации в киберпространстве. В свою очередь, киберпространство – это сложная среда, возникающая в результате взаимодействия людей, программного обеспечения и услуг в сети Интернет с помощью технологических устройств и подключенных к нему сетей, которые не существуют в какой-либо физической форме.

Международный союз электросвязи (ITU) [2]. Кибербезопасность – набор инструментов, политик, концепций безопасности, руководств, подходов к управлению рисками, действий, обучения, лучших практик, гарантий и технологий, которые можно использовать для защиты киберсреды, а также активов организации и пользователей. Активы организации и пользователей включают подключенные вычислительные устройства, персонал, инфраструктуру, приложения, услуги, телекоммуникационные системы и совокупность передаваемой и/или хранимой

информации в киберсреде. Кибербезопасность стремится обеспечить достижение и поддержание свойств безопасности организации и активов пользователя от соответствующих рисков безопасности в киберсреде.

NIST National Institute of Standards and Technology (Национальный институт по стандартизации и технологиям). Кибербезопасность – способность защищать и оборонять киберпространство от кибератак.

CNSS – Committee on National Security Systems (Комитет по системам национальной безопасности (США)). Кибербезопасность – предотвращение повреждения, защита и восстановление компьютеров, систем и услуг электронной связи, включая содержащуюся в ней информацию для обеспечения ее доступности, целостности и конфиденциальности.

В данных определениях есть общая мысль – не подразумевается разделение между преднамеренными и непреднамеренными действиями. Некоторые определения в качестве угроз определяют только виртуальные ресурсы (например, в стандарте ISO 27000), а другие (например, у НАТО) подразумевают, что угрозы могут носить как виртуальный, так и физический характер.

Стратегия кибербезопасности – документ, который фиксирует и определяет государственную политику, направленную на обеспечение безопасности государства в киберпространстве.

Киберстратегия США состоит из четырех частей и носит декларативный характер [3]:

1. «Защита американского народа, Родины и американского образа жизни». В этой части речь идет о безопасности федеральных сетей и критической информационной инфраструктуры. Также имеются и разделы о борьбе с киберпреступностью и улучшении отчетности о киберинцидентах.

2. «Содействие процветанию Америки». Здесь описаны принципы цифровой экономики, планы развития безопасного рынка технологий. А также заложены принципы сохранения США как лидера в создании новых технологий.

3. «Сохранение мира силой». В этой части изложены меры противодействия «неприемлемому» поведению в киберпространстве.

4. «Усиление американского влияния». Эта глава посвящена принципам работы безопасного и свободного Интернета, здесь же затронута проблема усиления киберпотенциала страны.

Иногда, вместо понятия «киберпространство», авторы стратегии используют понятие «сеть Интернет». Например, следующая цитата подчеркивает, как Интернет ценен для США: *«Америка создала Интернет и поделилась им со всем миром. Теперь мы должны убедиться в безопасности киберпространства для будущих поколений»*.

Буквально на днях (сентябрь 2023 г.) США приняли новую редакцию стратегии национальной кибербезопасности, носящую более прагматичный характер, направленный прежде всего на обеспечение безопасности критически важной инфраструктуры [4].

Цель стратегии описана в следующих пяти базовых принципов:

· Защита критически важной инфраструктуры, которая осуществляется с помощью применения минимальных требований к кибербезопасности в критически важных секторах экономики.

· Противодействие злоумышленникам в сети, их полное «разоружение». Здесь планируется задействовать потенциал частных компаний.

· Формирование сильных частных компаний, которые будут отвечать за безопасность и устойчивость киберпространства. Государство доверит ответственность за киберзащиту на более сильных игроков экономической системы. В результате такого снижения рисков слабые и наименее защищённые участники экосистемы будут освобождены от ответственности за последствия инцидентов кибербезопасности.

· Стратегические инвестиции в безопасное будущее и координация совместных действий всех субъектов экономического развития обеспечит стране ведущую роль в мире в области инноваций в сфере безопасной и устойчивой инфраструктуры и технологий нового поколения.

Создание взаимовыгодных партнерских отношений на международной арене для достижения общих целей: наращивания возможностей партнёров США противостоять киберугрозам как в мирное время, так и в кризисное.

**Роль и место системы национальной сертификации и стандартизации в реализации стратегии кибербезопасности США**

Механизмы контроля безопасности 800-53 Национального института стандартов и технологий (NIST), как правило, применяются к федеральным информационным системам США. Федеральные информационные системы обязаны проходить процедуру официальной оценки (сертификации) и авторизации, чтобы гарантировать достаточную степень защиты конфиденциальности, целостности и доступности информации в используемых информационных системах.

Правительства и корпорации поддерживают применение платформы кибербезопасности CSF (англ. – Cybersecurity Framework, CSF) [5], разработанной NIST, в качестве рекомендованных основных принципов для любой организации, независимо от сферы деятельности или размера. По результатам отчетов Gartner, в 2015 году 30% компаний в США использовали CSF, а к 2025 году планируется достижение 70% использования CSF. Начиная с 2016 г. все показатели Федерального закона США о модернизации систем информационной безопасности (FISMA) ставятся в зависимость от CSF. Компании в США обязаны внедрять CSF в свои практики.

Эпоха стремительного технологического развития задает свои важные направления в ИБ, например, безопасность для промышленной автоматизации и систем управления. В целях подтверждения защищенности (кибербезопасности) автоматизированных систем управления и промышленной автоматики необходимо выполнять сертификацию по стандарту ISA/IEC 62443. Чтобы поддерживать обеспечение безопасности систем автоматизации в рабочем состоянии необходимо, в первую очередь, противостоять заражениям вирусами и внедрению вредоносного ПО.

Серия стандартов ISA/IEC 62443 [6] разрабатывается комитетом ISA99 для использования в качестве национальных стандартов США и одобрена Международной электротехнической комиссией (IEC) для

международного применения. Основная цель стандарта ISA/IEC 62443-4-1-2018 – это требования к обеспечению безопасного жизненного цикла разработки и поддержки защищенных продуктов. В этом регламенте изложены принципы создания поставщиком безопасной инфраструктуры для работы АСУ, что затрагивает все этапы разработки системы информационных технологий, от первоначального проектирования до вывода из эксплуатации.

В стандарте ISA/IEC 62443 содержатся следующие требования:

· к проектированию,

· к безопасной реализации (программированию),

· к верификации и проверке подлинности,

· к управлению дефектами, управлению исправлениями и окончанию срока службы продукта с учетом безопасности.

Данный стандарт задает требования к процессу безопасной разработки продуктов, используемых в АСУ ТП. В основу документы положены 6 основных принципов:

· Безопасность периметра сети. Устанавливается контроль точек, где вредоносное ПО может проникнуть в систему автоматизации производства.

· Защита рабочих станций. В результате этих мер снижаются риски заражения рабочих станций.

· Управление учетными записями.

· Обновления безопасности.

· Резервное копирование и восстановление.

· Мониторинг безопасности и оценка рисков.

Ниже будут изложены рекомендации для компаний, работающих с персональными данными:

· Существенно снизить риски проникновения вредоносного программного обеспечения и предотвращать утечку данных.

· Обеспечить бесперебойную работы сети предприятия, наладить качественную связь между подразделениями.

· Обеспечить доверие клиентов.

· Снизить расходы, а также избежать риски инцидентов ИБ на этапе внедрения ПО и на других этапах жизненного цикла систем автоматизации.

Какие же компании, в первую очередь, должны придерживаться требований к программе обеспечения защищенности (кибербезопасности) согласно данного стандарта? Это компании поставщики услуг IACS (Instruments and Automatic Control System), а также компании, которые планируют расширяться и предоставлять услуги и товары в США и странах ЕС.

Рассмотрев специфику законодательства США в области стандартизации и сертификации продуктов и систем кибербезопасности, далее перейдём к анализу рынка продаж этих решений на таможенной территории страны и за её пределами.

**Продажи решений по кибербезопасности. Финансовый анализ**

Кибербезопасность уже некоторое время является главной составляющей в расходах ИТ-департаментов, опережая долгосрочные инвестиции в такие сферы, как искусственный интеллект и цифровую трансформацию бизнеса, которые, в свою очередь, нуждаются в обеспечении информационной безопасности. Данное стечение обстоятельств вызвано в первую очередь разрушительным ущербом от программ-вымогателей и киберугроз, направленных против цепочек поставок программного обеспечения и критической инфраструктуры предприятий. Киберугрозы – это попытки через Интернет нарушить работу или повредить информационные системы и взломать критически важную информацию с помощью шпионских программ, вредоносных программ и фишинговых атак. Учитывая ущерб, который может нанести нарушение интеллектуальной собственности, репутации и доходам компании (не говоря уже о крупных штрафах в соответствии с законами о конфиденциальности данных), компании вкладывают значительные средства в развитие корпоративной безопасности [7].

Рынок кибербезопасности включает в себя доходы, полученные от продажи продуктов и услуг.

Отчет правительства США о рынке кибербезопасности предоставляет разнообразные данные по конечным пользователям (подготовлен ЦРУ, Министерством обороны и Министерством внутренней безопасности), местам развертывания (локальное и облачное) и видам продуктов (услугам и решениям). Он также содержит в себе углубленный анализ текущих трендов и проблем.

Прежде всего, рост рынка обусловлен инновационными изменениями в пользовательском интерфейсе межсетевых экранов (МЭ). Так называемые брандмауэры предоставляют пользователям улучшенную защиту с помощью формирования черных списков, фильтрации URL-адресов и автоматической блокировки от угроз со стороны злоумышленников. Поставщики межсетевых экранов могут использовать подобные методы противодействия киберугрозам на проникновение к внутренней сети, путём создания демилитаризованной зоны DMZ.

В последнее время на рынке средств кибербезопасности появились межсетевые экраны нового поколения (Next-Generation Firewall, NGFW), которые, кроме основных функций брандмауэра, имеют еще и дополнительные функции, такие как:

· контроль приложений;

· DPI (Deep Packet Inspection, проверка пакетов на уровне приложений);

· IPS (предотвращение вторжений);

· веб-фильтрация (контроль URL-адресов, к которым обращаются пользователи);

· аутентификация пользователей.

Также к штатным функциям МЭ могут быть дополнительно агрегированы опции безопасности с использованием искусственного интеллекта (ИИ) и машинного обучения (МО), такие как:

· *EDR* (Endpoint Detection and Response). Смысл этой функции в обнаружении неизвестных вредоносных программ, автоматической классификации любых угроз и самостоятельного реагирования на них. Все данные затем передаются в центр управления. Используя общую базу знаний, ИИ принимает решения по противодействию угрозам. Также с помощью ИИ можно выявить и внутренние угрозы.

· *NDR* (Network Detection and Response) – аналитические платформы, которые служат для обнаружения атак на сетевом уровне, а затем оперативно реагируют на них. Как это работает? С помощью накопленной статистики и базы знаний об угрозах появляется возможность выявлять угрозы в сетевом трафике и реагировать на них, с помощью изменений в конфигурации сетевых устройств и шлюзов. Некоторые продукты такого плана специализируются на защите облачных провайдеров. Применяются NDR и для анализа почтового трафика на предмет фишинга.

· *UEBA* (User and Entity Behavior Analytics) – системы поведенческого анализа пользователей и информационных сущностей. Смысл работы подобных систем состоит в том, чтобы обнаружить необычное поведение и применить полученные данные для фиксирования внутренних и внешних угроз. *UEBA* помогают выявить аномалии в поведенческих моделях. Это может быть выражено как отклонение от нормы или соответствие паттерну угрозы. Далее происходит классификация обнаруженных аномалий с помощью ИИ. Основные сферы применения метода – это мониторинг и управление доступом, антифрод, защита конфиденциальных данных, проверка соблюдения регламентов и нормативных актов.

· *TIP* (Threat Intelligence Platform) – платформы раннего детектирования угроз и реагирования на них. Принцип действия таких платформ – это сбор огромного количества самых разных данных (*Data Lake*) и определение индикаторов компрометации (*IoC)*. В чем-то TIP напоминает работу SIEM, но TIP нацелена на внешние источники данных и внешние угрозы.

· *SIEM* (Security Information and Event Management) – предназначены для мониторинга информационных систем. В режиме реального времени SIEM производят анализ событий безопасности. Информация в SIEM стекается из сетевых устройств, средств защиты информации, ИТ-сервисов, инфраструктуры систем и приложений. Затем происходит обнаружение инцидентов ИБ.

· *SOAR* (Security Orchestration and Automated Response) – это системы, которые не просто находят угрозы информационной безопасности, они занимаются автоматизацией реагирования на инциденты.

· *AS* (Application Security). Главный смысл работы таких систем – это выявление угроз безопасности прикладных приложений, а затем их устранение. С помощью решений ИИ происходит сбор информации об уязвимостях, атаках и заражениях. Затем на основании результатов полученной информации выполняются автоматические сценарии защитных действий. Это может быть сканирование на уязвимости, применение новых правил защиты для веб-приложений, выявление новых угроз, анализ модели рисков.

· *AF* Антифрод (Antifraud) – системы, предназначенные для борьбы с мошенничеством в финансовых учреждениях в режиме реального времени. С помощью искусственного интеллекта можно выявить нарушения в бизнес-процессах компании. А затем можно быстро отреагировать на потенциальное преступление или уязвимость какого-либо бизнес-процесса.

· *ZTNA* (Zero Trust Network Access) – системы доступа с «нулевым доверием». Термин «нулевое доверие» понимается прямо в буквальном смысле. В такой системе ни один пользователь или устройство не считаются надежными, ни одна транзакция не считается безопасной. Всегда происходит предварительная проверка авторизации пользователя и устройства.

· *DLP* (Data Loss Prevention) – системы, которые предназначены для предотвращения потери/утечки данных. Они обычно работают с внутренними угрозами в компании и противодействуют инсайдерам. Принцип DLP-системы заключается в анализе потоков данных, пересекающих периметр корпоративной системы. Применяется технология контентного анализа на основе алгоритма Байеса и метода опорных векторов.

Применение ИИ в таких системах особенно актуально, так как позволяет быстро адаптироваться к изменению логики и различных метрик бизнес-процессов, а также использовать лучшие практики в индустрии кибербезопасности. Для всех типов данных систем технологии искусственного интеллекта позволяют увеличить эффективность детектирования неизвестных угроз. Данные новшества способствуют развитию рынка как межсетевых экранов, так и интеллектуальных средств информационной безопасности в ближайшие годы [8].

Ожидается, что до 2033 года технология межсетевых экранов на основе ИИ и МО в США станет главенствующей и ее доля составит около 78,6% в Северной Америке.

В США поставщики NGFW сосредоточены на развитии и продвижении своих систем обнаружения и предотвращения вредоносного проникновения для выявления и последующего анализа кибератак (IPS/IDS). Эти крупные компании ориентируются на малые и средние бизнесы, которые стремятся обеспечить безопасность своих приложений, хранящихся в облаке, и предлагают им значительно более низкие цены [9].

В марте 2019 года было объявлено об открытии офиса кибер- и энергетической безопасности в США с выделением бюджета в размере 96 миллионов долларов США.

Следует отметить, что законодательные и регуляторные процессы на федеральном уровне штатов также способствуют повышению расходов на кибербезопасность, создавая условия для разумного регулирования данной сферы. Например, в штате Луизиана в 2021 году был принят закон об обязательном уведомлении в случае выявления возможной уязвимости в решениях от поставщиков управляемых услуг, работающих на государственный сектор экономики (Louisiana Act 117 – Senate Bill 273). В таком случае компаниям необходимо приобретать программы безопасности, которые будут не только отражать потенциальные кибератаки, но также и фиксировать возникновение потенциальных рисков [9].

В 2022 финансовом году расходы Министерства внутренней безопасности США на гражданскую кибербезопасность составили 2,4 миллиарда долларов США. Министерство юстиции выделило около 1,2 миллиарда

долларов США на соответствующие инвестиции в кибербезопасность. Общие расходы финансовых директоров государственных агентств на кибербезопасность (исключая Министерство обороны) составили 9,3 миллиарда долларов США [10].

На 2023 финансовый год президент США запросил 2,5 миллиарда долларов на кибербезопасность. Это на 18% выше, чем в 2022 году. К этому следует добавить, что 11,2 миллиарда долларов было выделено на развития кибербезопасности Пентагона. Это на 8% больше предыдущего запроса администрации Байдена [11].

Соединенные Штаты являются лидером по продажам продуктов кибербезопасности наряду с Израилем.

На 2023 год объем рынка кибербезопасности США оценивается в 73,41 миллиарда долларов США и, как ожидается, он достигнет отметки в 108,31 миллиарда долларов США к 2028 году. Среднегодовой рост составит 8,09% в течение прогнозируемого периода (2023-2028 годы).

В число ключевых игроков в области решений для отраслевой кибербезопасности в США входят Fortinet, Intel Sequrity, Dell, Cisco, IBM [12].

Основными участниками рынка коммерческой кибербезопасности являются: Cisco System, Nexusguard Limited, BAE Systems Intelligence & Security, Ixtel Technologies, Argus Cyber Security, McAfee, Root9B Technologies, Symantec Corp, Check Point Software Technology, Cato Networks и PhishMe In [13].

Стоит уделить внимание на тот факт, что на рынке США становится все более популярным продукт, основанный на технологии искусственного интеллекта – Darktrace от одноименной британской компании (г. Кембридж). Компания представляет систему распознания киберрисков по нетипичной активности в сетях, к которым подключен компьютер. Установка системы Darktrace требует выезда специалиста на место ИКТ-инфраструктуры компании-заказчика, также компания проводит обучение внутренних ИТ-специалистов по работе с системой [14].

Другая компания в сфере кибербезопасности, Horizon3.ai, базирующаяся в Калифорнии, привлекла инвестиции в размере 5 миллионов долларов США в рамках раунда инвестиций серии А, который возглавил SignalFire.

Fortinet – это второй по размеру выручки игрок в секторе кибербезопасности США (уступает только Palo Alto), также ежегодно получает инвестиции размером в десятки миллионов долларов. Стоит отметить, что Fortinet является самым маржинальным игроком в секторе кибербезопасности и сохраняет высокий темп прироста прибыли в размере 30% несколько лет подряд.

В то время как большинство сегментов IT сектора США значительно замедляются, рынок кибербезопасности по-прежнему показывает опережающий рост: за 2023 год рост рынка составит 13,2%, а к 2026 году объём рынка вырастет до $280 млрд. (+80% с текущих уровней). Бизнесы таких компаний как Fortinet и Palo Alto хорошо диверсифицированы как по клиентам (от малого до крупного бизнеса) и конечным индустриям, так и географически (самую крупную долю в выручки занимает США с 28%) [15].

Выручка компании Fortinet, Inc. за 2022 год составила 4,42 миллиарда долларов США. Большая часть – 1,78 миллиардов долларов США – была получена из сектора сетевой безопасности, который за год до этого принёс компании 1, 25 миллиарда долларов США (таблица 1).

Таблица 1 - Выручка компании Fortinet, Inc. по видам деятельности

DOI: https://doi.org/10.18454/itech.2024.2.2.1

| Вид деятельности | 2020 год, млн. дол. США | 2021 год, млн. дол. США | 2022 год, млн. дол. США |
|---|---|---|---|
| Устройства сетевой безопасности | 916,4 | 1250 | 1780 |
| Услуги по безопасности | 918,7 | 1130 | 1430 |
| Техническая поддержка | 759,3 | 962,2 | 1210 |

*Примечание: по ист. [15]*

Что касается деления выручки по странам, то на США приходится наибольшая доля выручки за последние несколько лет. Несмотря на то, что общий объем выручки по Европе и Африке, превышает объем выручки по США. В таблице 2 представлены уровень выручки по странам компании Fortinet, Inc. [15].

Таблица 2 - Выручка компании Fortinet, Inc. по странам

DOI: https://doi.org/10.18454/itech.2024.2.2.2

| Страна | 2020 год, млн. дол. США | 2021 год, млн. дол. США | 2022 год, млн. дол. США |
|---|---|---|---|
| США | 813,3 | 1010 | 1320 |
| Европа, Южная и Средняя Африка | 991,9 | 1280 | 1690 |

| | | | |
|---|---|---|---|
| Другие страны Америки | 263,9 | 352 | 460 |
| Страны Азии | 525,3 | 707,5 | 940,6 |

*Примечание: по ист. 15*

При этом стоит заметить, что росту рынка препятствует высокая стоимость внедрения решений по кибербезопасности. Сюда входят лицензирование программного обеспечения, настройка систем, обучение и расходы на обслуживание. Наем ИТ-персонала и проведение обучения увеличивают общие затраты на внедрение новых технологий. Кроме того, скрытые затраты, такие как развитие корпоративной культуры кибербезопасности и различные тренинги, еще больше увеличивают финансовые вложения. Постоянный мониторинг и устранение новых угроз приводят к росту расходов на кибербезопасность у компаний любых размеров, и это является ключевым фактором роста рынка в ближайшие 5 лет.

По прогнозам, выручка в сегменте программного обеспечения для улучшения систем безопасности на рынке США будет постоянно увеличиваться в период с 2023 по 2026 год. В общей сложности данный сегмент вырастет на 5,7 миллиарда долларов США (+21,33 процента). Согласно этому прогнозу, в 2026 году выручка всех ключевых игроков увеличится, третий год подряд достигнув рекордного показателя в 32,44 миллиарда долларов США. Примечательно, что доходы компаний, работающих в секторе кибербезопасности постоянно росли в течение последних лет [16].

Развитие рынка кибербезопасности в США находится в зависимости от нескольких ключевых факторов, таких как, рост продаж межсетевых экранов, внедрения гибридной модели проектирования решений кибербезопасности и увеличение бюджета на ИТ-безопасность во многих компаниях. Принятие верных решений в области кибербезопасности позволяют правительству США сохранять конфиденциальность данных путем мониторинга, обнаружения, составления отчетов и противодействия угрозам кибербезопасности [16]. Согласно указу президента США от 27 марта 2023 года, государственным организациям запрещено использовать коммерческое шпионское программное обеспечение, которое создаёт угрозу национальной безопасности.

**Заключение**

Изучив отчеты и статистику, предоставленную в этой статье, можно сделать вывод, что рынок корпоративной безопасности обширен и охватывает целый ряд технологий и систем, которые постоянно требуют доработок и внимания со стороны поставщиков товаров и услуг по кибербезопасности. Некоторые поставщики предлагают множество продуктов, в то время как другие специализируются только на одном или двух. Чтобы выбрать потенциального поставщика для бизнеса, сначала необходимо внимательно изучить потребности компании и бизнес-процессы, прежде чем делать выбор в пользу какого-то из продуктов.

Научная новизна работы заключается в выявлении взаимосвязи между такими теоретическими понятиями, как «киберстратегия государства», «кибербезопасность», «киберпространство» и др. положениями международных стандартов и совершенно практическими показателями объемов продаж на рынке продуктов и систем кибербезопасности. В статье приводятся исследования на примере США – самого крупного рынка в сфере кибербезопасности. Показаны примеры регулирования столь специфического рынка (как рынок систем кибербезопасности) на стратегическом и макроэкономическом уровнях (разработка стратегий правительства США) и на уровне микроэкономики (выход на рынок коммерческих компаний и вывод их продуктов). Статья будет полезна российским специалистам, исследователям и бизнесменам в сфере ИБ для оценки рыночных возможностей самого крупного конкурента в области кибербезопасности.

**Конфликт интересов**

Не указан.

**Рецензия**

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

**Conflict of Interest**

None declared.

**Review**

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

**Список литературы / References**

1. Top cybersecurity companies. — URL: https://www.esecurityplanet.com/products/top-cybersecurity-companies/ (accessed: 03.09.2023).

2. Cybersecurity market. — URL: https://www.canalys.com/newsroom/cybersecurity-market-2022/ (accessed: 03.09.2023).

3. Cyber security as a service market. — URL: https://www.mordorintelligence.com/ru/industry-reports/cyber-security-as-a-service-market (accessed: 03.09.2023).

4. Us government spending cyber security department. — URL: https://translated.turbopages.org/proxy_u/en-ru.ru.4d2a43f8-64f760a0-e6246765-74722d776562/https/www.statista.com/statistics/697244/us-government-spending-cyber-security-department/ (accessed: 03.09.2023).

5. О новой американской стратегии кибербезопасности. — URL: https://zavtra.ru/blogs/o_novoj_amerikanskoj_strategii_kiberbezopasnosti (дата обращения: 03.09.2023).

6. Industry cybersecurity. — URL: https://medium.com/@yooniiouy/industry-cybersecurity-solution-market-2023-2029-covid-19-impact-analysis-206b6abee9af (accessed: 03.09.2023).

7. Statistics. — URL: https/www.wallstreetzen.com/stocks/us/nasdaq/csco/statistics (accessed: 06.09.2023).

8. Commercial cyber security market. — URL: https://www.marketwatch.com/ press-release/commercial-cyber-security-market-2023-share-industry-size-growth-opportunities-technologycal-advancement-and-forecast-to-2030-cisco-system-nexusguard-limited-bae-systems-intelligence-security-ixtel-technologies-2023-06-17 (accessed: 06.09.2023).

9. Выручка Fortinet. — URL: https://www.tinkoff.ru/invest/social/profile/TAUREN_invest/09236ecc-59d3-404e-a05b-736b42a8495b/ (дата обращения: 06.09.2023).

10. Government cyber security market. — URL: https://www.technavio.com/report/government-cyber-security-market-in-us-industry-analysis (accessed: 03.09.2023).

## Список литературы на английском языке / References in English

1. Top cybersecurity companies. — URL: https://www.esecurityplanet.com/products/top-cybersecurity-companies/ (accessed: 03.09.2023).

2. Cybersecurity market. — URL: https://www.canalys.com/newsroom/cybersecurity-market-2022/ (accessed: 03.09.2023).

3. Cyber security as a service market. — URL: https://www.mordorintelligence.com/ru/industry-reports/cyber-security-as-a-service-market (accessed: 03.09.2023).

4. Us government spending cyber security department. — URL: https://translated.turbopages.org/proxy_u/en-ru.ru.4d2a43f8-64f760a0-e6246765-74722d776562/https/www.statista.com/statistics/697244/us-government-spending-cyber-security-department/ (accessed: 03.09.2023).

5. O novoj amerikanskoj strategii kiberbezopasnosti [On the new U.S. cybersecurity strategy]. — URL: https://zavtra.ru/blogs/o_novoj_amerikanskoj_strategii_kiberbezopasnosti (accessed: 03.09.2023). [in Russian]

6. Industry cybersecurity. — URL: https://medium.com/@yooniiouy/industry-cybersecurity-solution-market-2023-2029-covid-19-impact-analysis-206b6abee9af (accessed: 03.09.2023).

7. Statistics. — URL: https/www.wallstreetzen.com/stocks/us/nasdaq/csco/statistics (accessed: 06.09.2023).

8. Commercial cyber security market. — URL: https://www.marketwatch.com/ press-release/commercial-cyber-security-market-2023-share-industry-size-growth-opportunities-technologycal-advancement-and-forecast-to-2030-cisco-system-nexusguard-limited-bae-systems-intelligence-security-ixtel-technologies-2023-06-17 (accessed: 06.09.2023).

9. Vyruchka Fortinet [Fortinet's revenue]. — URL: https://www.tinkoff.ru/invest/social/profile/TAUREN_invest/09236ecc-59d3-404e-a05b-736b42a8495b/ (accessed: 06.09.2023). [in Russian]

10. Government cyber security market. — URL: https://www.technavio.com/report/government-cyber-security-market-in-us-industry-analysis (accessed: 03.09.2023).