постепенно меняться, особенно когда по прошествии первых лет переговоров все более очевидным становилось ощущение их углубляющегося кризиса.

Таким образом, сложившаяся в ВТО после Уругвайского раунда система принятия решений близка к исчерпанию своего ресурса эффективности и в перспективе вряд ли будет жизнеспособной. Очевидным симптомом ее несрабатывания становится отсутствие в течение длительного времени (конкретно в период 2002–2012 гг.) прогресса на переговорах Доха-раунда.

Изложенное выше лишь подтверждает, что потребность институционального реформирования ВТО стала актуальной, однако решение данного вопроса потребует значительных усилий и времени.

Литература

1. 25-летие ВТО: юбилей под знаком кризиса [Электронный ресурс]. – Режим доступа: https://www.dw.com/ru/. – Дата доступа: 10.04.2021.

2. Портанский, А. П. Перспективы и риски трансформации системы регулирования мировой торговли: глобальный и мегарегиональный аспекты. – Москва, 2019. – 365 с.

3. Три кризиса ВТО [Электронный ресурс]. – Режим доступа: https://econs.online/articles/ekonomika/tri-krizisa-vto/. – Дата доступа: 08.04.2021.

Проблема кибербезопасности в цифровой мировой экономике

Романовский З. В., студ. IV к. БГУ,
науч. рук. Головенчик Г. Г., канд. экон. наук, доцент

Киберпреступления стали повседневной проблемой как для бизнеса, так и для общества. Статистика киберпреступности свидетельствует о значительном росте утечек данных и взломов, большинство из которых связано с устройствами на рабочем месте. Так как люди все больше полагаются на цифровые технологии во всех областях экономики и общественной жизни, многим организациям необходима эффективная стратегия, которая поможет выявлять уязвимости для киберугроз и решать проблемы в области кибербезопасности.

Необходимо понимать, что киберпреступность с каждым днем становится все более изощренной, что еще усугубляется массовым распространением технологий искусственного интеллекта, больших данных, облачных вычислений и интернета вещей, которые все чаще используются в бизнес-процессах и производственной сфере. Инновационные цифровые технологии предоставляют все больший спектр возможностей для достижения большего

количества целей, но в то же время делают бизнес-систему более уязвимой для кибератак. Более того, некоторые цифровые технологии уже активно используются киберпреступниками, например, искусственный интеллект, который применяется организациями для обнаружения аномалий и предотвращения кибератак. Хакеры научились использовать технологии искусственного интеллекта и машинного обучения для персонализации атак, чтобы точно знать, кого и когда можно взламывать в конкретной организации. Благодаря этому нарушения данных и кибератаки становятся все более эффективными и влекут за собой огромные издержки, отрицательно влияя на непрерывность бизнеса.

Самое важное: проблема заключается уже не в том, будут ли кибератаки происходить вообще, а в том, когда они произойдут и как организация сможет быстро отреагировать на них и восстановиться. Вот почему вопрос кибербезопасности настолько актуален на сегодняшний день.

Также крайне важно иметь представление о том, какие наиболее распространенные типы кибератак существуют и откуда они берутся. В отчете Cyberthreat Defense Report 2020 [1] исследовательской консалтинговой компании Cyber Edge Group указано, что наибольшую озабоченность у руководителей компаний вызывает вредоносное ПО, на втором месте – фишинг, далее следуют программы-вымогатели, атаки по захвату учетных записей и отказ в доступе.

Наиболее распространенными кибератаками, с которыми сталкиваются американские компании, являются фишинг (38%), сетевое вторжение (32%), непреднамеренное раскрытие информации (12%), кража/потеря устройств или записей (8%) и неправильная конфигурация системы (5%) [2].

Согласно исследованию Comparitech 2020, самыми кибербезопасными странами в мире, основанному на оценке уязвимости к кибератакам, являются Дания (6,72), Швеция (8,40), Германия (9,39), Ирландия (9,40) и Япония (9,46). С другой стороны, наименее кибербезопасными странами в мире, исходя из оценки уязвимости к кибератакам, являются Алжир (48,99), Таджикистан (48,54), Туркменистан (48,39), Сирия (44,51) и Иран (43,48) [3].

В контексте кибербезопасности не стоит также забывать о такой глобальной проблеме, как пандемия COVID-19, которая затронула все сферы социально-экономических отношений, в том числе и киберпространство. Эпидемия открыла для киберпреступников возможности «охоты» на множество новых жертв: индустрию здравоохранения, безработных, сотрудников, работающих дистанционно, и многих других. Например, из-за пандемии подтвержденные утечки данных в сфере здравоохранения в 2020 г. увеличились на 58% [4]; согласно информации Atlasvpn, только за первые семь месяцев 2020 г. американцы потеряли более 97,4 млн долл. из-за мошенничества с COVID-19 (включая обман интернет-магазинов; создание мошеннических

сайтов, продающих добавки, маски, даже не одобренные FDA вакцины; мошенничество с возвратом денег за поездки и отпуска) и стимулирующими чеками [5].

Таким образом, по результатам проведенного анализа можно сделать вывод о том, что проблема обеспечения кибербезопасности крайне важна на сегодняшний день. С появлением все большего количества цифровых технологий становится труднее поддерживать безопасность, так как хакеры научились адаптироваться к постоянно прогрессирующим технологиям киберзащиты. Поэтому для обеспечения безопасности компаний необходимы эффективные стратегии кибербезопасности, основанные на использовании инновационных технологий искусственного интеллекта и машинного обучения.

Литература

1. Cyberthreat Defense Report 2020 [Электронный ресурс]. – Режим доступа: https://www.isc2.org/-/media/ISC2/Research/Cyberthreat-Defense-Report/CyberEdge-2020-CDR-Report-v10.ashx. – Дата доступа: 21.04.2021.

2. Most common cyber attacks experienced by companies in the United States in 2019 // Statista [Электронный ресурс]. – Режим доступа: https://www.statista.com/statistics/293256/cyber-crime-attacks-experienced-by-us-companies/. – Дата доступа: 22.04.2021.

3. 119 Impressive Cybersecurity Statistics: 2020/2021 Data and Market Analysis [Электронный ресурс]. – Режим доступа: https://financesonline.com/cybersecurity-statistics/. – Дата доступа: 22.04.2021.

4. 2020 Data Breach Investigations Report [Электронный ресурс]. – Режим доступа: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf. – Дата доступа: 21.04.2021.

5. Over 150,000 COVID-related fraud reports submitted to the US Government YTD [Электронный ресурс]. – Режим доступа: https://atlasvpn.com/blog/over-150-000-covid-related-fraud-reports-submitted-to-the-us-government-ytd. – Дата доступа: 22.04.2021.

Конструкция «спонтанного порядка» как альтернатива государственному регулированию экономики в теории Ф. Фон Хайека

Сащеко Р. С., аспирант БГУ,
науч. рук. Барсук И. А., канд. филос. наук, доцент

Одной из центральных фигур в мировой социально-экономической мысли XX века по праву считается австро-британский экономист, представитель новой австрийской школы Ф. фон Хайек (1899–1992). В своих