

4. Коммерсантъ: Госдума одобрила наказание за фейки о коронавирусе: вплоть до 5 лет лишения свободы [Электронный ресурс]. – Режим доступа: <https://www.kommersant.ru/doc/4309307>. – Дата доступа: 28.01.2022.

5. Минченкова, О. Ю. Роль и значение интернета в развитии гражданского общества / О. Ю. Минченкова, Н. В. Федорова, В. Г. Макеев // Вестник РГГУ. – Серия Экономика. Управление. Право. – 2021. – №1. – С. 8–15.

6. Пугачев, В. П. Глобалистский тоталитаризм. Социальные мутации цифрового капитализма: формирование человека и манипулятивные технологии управления / В. П. Пугачев. – М. : URSS, 2022. – 232 с.

7. Пугачев, В. П. Глобалистский тоталитаризм – тренд развития цифрового общества / В. П. Пугачев // Свободная мысль. – 2021. – № 4. – С. 5–18.

8. Руф, Ю. Н. Возможности внедрения системы социального рейтинга в России в условиях цифровизации / Ю. Н. Руф, Д. В. Каримова // Вопросы инновационной экономики. – 2020. – № 2. – С. 881–890.

9. Tadvise.ru: 2021: Контракт на обновление СТАТС с компанией «Программный продукт». [Электронный ресурс]. – Режим доступа: [https://www.tadviser.ru/index.php/Проект:Информационная_система_мониторинга_и_анализа_интернет-активности_\(ИС_СТАТС\)](https://www.tadviser.ru/index.php/Проект:Информационная_система_мониторинга_и_анализа_интернет-активности_(ИС_СТАТС)). – Дата доступа: 28.01.2022.

А.А. Иванов,
студент НГЛУ им. Н.А. Добролюбова (Нижний Новгород, Россия)
Научный руководитель – к.полит.н. Е.М. Рогожина

ЛОББИСТСКАЯ ДЕЯТЕЛЬНОСТЬ В СФЕРЕ ЦИФРОВОЙ БЕЗОПАСНОСТИ

За последние два десятилетия огромное развитие получили информационные технологии и интернет, а сам процесс внедрения и распространения данных технологий получил название «цифровизация». С начала пандемии COVID-19 данная тенденция получила своё значительное развитие в связи с изменением ряда условий жизни общества, трансформацией процесса обеспечения должного уровня цифровой безопасности как государственного сектора, так и частных компаний и гражданского сектора, а обеспечение цифровой безопасности стало одним из важнейших приоритетных условий развития каждого, кого касается данная проблема. Согласно исследованию Check Point Research (CPR), общее количество атак в корпоративных сетях в 2021 г. увеличилось на 50 % в неделю по сравнению с 2020 г., а рост числа кибератак на правительственный сектор увеличился на 47 % в неделю [9]. Сектор экономики потерял множество средств из-за кибератак. Все эти проблемы стали накладываться на уже имеющиеся трудности, что привело к значительному росту лоббистской деятельности в данной области.

К причинам роста лоббистской активности можно отнести то, что компании резко реагируют на утечку данных, а также то, что государственные

должностные лица меняют законы о конфиденциальности и безопасности. Все это вынуждает компании полностью менять собственную систему рабочей деятельности. Необходимо упомянуть, что законопроекты вырабатываются при условии диалога между компаниями и правительствами, компании вместе с поставщиками услуг цифровой безопасности стремятся к заключению выгодных контрактов.

Серьезность проблем, вызванных пандемией COVID-19, заставила ускорить принятие решений и реакцию на современные проблемы, что негативно отразилось на компаниях, которые ежемесячно стали тратить миллионы долларов на лоббирование. С другой стороны, по данным немецкого журнала *Der Spiegel*, транснациональные корпорации благодаря пандемии COVID-19 получили прибыль в размере 400 млрд. долларов, хотя при этом прибыли более мелких компаний сократилось на 89 % [11]. Ответной реакцией правительств разных стран была инициатива по старту всемирной налоговой реформы с минимальной ставкой корпоративного налога в 15 %, а вступить в силу он должен будет в 2023 г. Все эти причины неразрывно связаны с началом лоббистской деятельности в сфере цифровой безопасности, так как государственный сектор потерял миллиарды долларов и правительства обратились за помощью к экспертным знаниям. Представители ТНК не готовы к изменению ситуации не в их пользу, поэтому началась работа над новыми законодательными инициативами, а лоббисты влияют на процесс принятия решений в законодательных и исполнительных ветвях власти. Сейчас же важным фактором того, как человечество преодолет кризис цифровой безопасности, является взаимодействие между правительством и лоббистскими организациями. Именно в этом направлении стало развиваться государственно-частное партнерство, благодаря которому могут быть минимизированы расходы бюджета за счет мотивации бизнеса [2, с. 282].

Благодаря лоббистской деятельности технологические компании понимают, обладают ли государственные органы достаточной информацией по цифровым технологиям, чтобы формировать направление политики. Например, киберкомпания США и Правительство Великобритании добились сотрудничества для решения проблем цифровой безопасности с дальнейшим поиском инновационных решений [12]. Благодаря эффективному сотрудничеству между компаниями и организациями появился проект Закона США об инновациях и конкуренции 2021 г. (находится на рассмотрении), который предусматривает выделение 110 миллиардов долларов на исследования в области базовых и передовых технологий в течение пяти лет [7]. Кроме того, за последние годы наблюдается рост лоббистской деятельности в США.

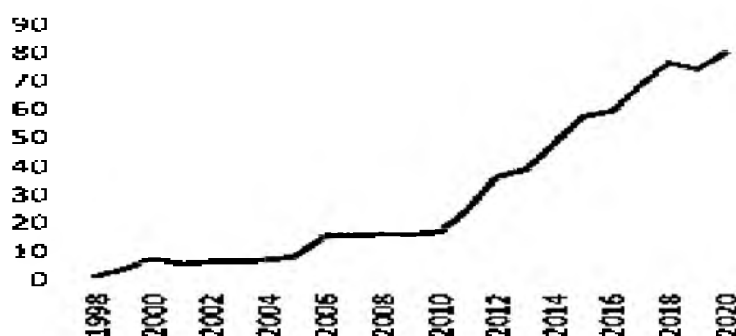


Рисунок 1. Лоббирование в США в сфере ИКТ

США – это центр передовых технологических компаний, на которые и совершаются массовые кибератаки с целью получения личных и платежных данных работников и пользователей. Любая кибератака сильно бьет по репутации каждой компании, и лоббизмом приходится пользоваться, чтобы добиться изменения законодательства, которое ставит компании в ограниченные рамки действия. Благодаря этому компаниям удалось добиться увеличения срока отчетности с 24 часов до 72, так как за 24 часа грамотно оценить ситуацию и представить отчет о кибератаке невозможно. Другим странам необходимо последовать примеру США и дать возможность высказывать свои решения на государственном уровне, а не только в рамках платформ, созданных для обмена мнениями, которые имеют небольшое политическое влияние на принятие законодательных инициатив.

К одной из самых крупных лоббистских групп, представляющей ведущие технологические компании, относится Совет по безопасности цифровой экономики, созданный в 2018 г. Его целями являются борьба с глобальными угрозами кибербезопасности и содействия экономическому росту. К партнерам и членскому составу Совета относятся представители таких телекоммуникационных компаний, как Samsung, Ericsson, Intel, Akamai. Для Совета главной угрозой являются ботнеты, способные вывести Интернет из рабочего состояния [8]. Каждый год Совет публикует обновленные версии международных руководств по безопасности Интернета вещей, чтобы способствовать эффективному развитию диалога между правительством и представителями других лоббистских групп. Однако терминология и ключевые понятия в частном и правительственном секторах сильно различаются, ведь каждый из них опирается на свои собственные методы, кроме моментов, когда функционирование и деятельность частного сектора регламентируются законом. Здесь можно сделать вывод о том, что в ходе анализа руководств было выявлено, что они опираются как на официальные документы правительства в сфере цифровой экономики и цифровой безопасности, так и на регламентирующие документы частных организаций. Без внимания также не остаются и децентрализованные организации, представляющие собой систему взаимодействующих структур, методов и механизмов государственного, муниципального, общественного и бизнес управления [3, с. 17]. Их влияние

заметно возросло в последние годы, что является результатом увеличения лоббистской деятельности, порождающей все новые взаимозависимости между компаниями и правительствами. Например, ENISA, чье влияние значительно увеличилось в годы пандемии COVID-19, именно в это время увеличил лоббистскую активность. Стоит отметить, что, несмотря на все усилия, Совет не справился со своей главной задачей – гармонизацией отношений между организациями и правительствами. Проблемы возникают внутри руководства и исполнительного консультативного совета, ведь их представители пытаются обеспечить продвижение собственных интересов, чтобы увеличить своё влияние на рынке. Из-за этого процесс принятия решения занимает больше времени, чем нужно. Подобное, на наш взгляд, является недопустимым, особенно в условиях, когда ожидается быстрая реакция на современные вызовы. А сами политики не всегда принимают во внимание мнение руководства Совета, предпочитая слушать экспертов из компаний, с которыми государства активно сотрудничают, ожидая от них получить нормативные подходы со ссылками на общепринятые межгосударственные сертификации и нормативно-правовые акты, которые Совет не всегда может предоставить. Эти примеры демонстрируют целостную картину взаимодействия компаний и лоббистских организаций, которые все ещё накапливают свою силу.

Наиболее успешным примером лоббистской деятельности является политика Amazon и наем Дж. Карни, бывшего пресс-секретаря Белого Дома, который провел гигантскую лоббистскую политику, сокрушившую законодательство в сфере конфиденциальности [5]. Дж. Карни смог убедить законодателей принять закон конфиденциальности, разработанный Amazon. Лоббизм направлялся за снятие ограничений, заставлявших компании раскрывать данные о потребителях. Несомненно, успех Amazon связан с их крупным влиянием на международные отношения и наличием большого количества пользователей, выступающих за неприкосновенность частной жизни. Кроме того, приглашение человека, разбирающегося в политике и пользующегося авторитетом, было отличным решением, так как зачастую в лоббизме в сфере цифровой безопасности участие принимают люди, мало разбирающиеся в выстраивании успешного диалога с правительствами. Не стоит исключать также ведущую роль Amazon в сфере ИКТ. Можно заключить, что некоторые деловые круги обладают высокой степенью авторитета в реализации своих желаний на государственном уровне [6].

С развитием цифровизации свое влияние стали набирать digital-инструменты, организованные электронные краудсорсинговые площадки, при помощи которых государство аккумулирует общественные инициативы, направленные на изменение внутренней и внешней политики [4, с. 55]. А граждане в таком случае будут лояльными по отношению к государственным структурам [1]. Однако, не увидев эффективных результатов, граждане остаются недовольными, особенно когда речь заходит об утечке данных или кибератаках, подорвавших финансовое положение фирм, в которых они работают. В любом

случае, коммуникационная стратегия между государственными учреждениями и гражданами должна присутствовать, но только при реагировании на возможные кибератаки и в случаях, когда правительство делится важными сообщениями с гражданами. Ведь данная работа занимает много времени, так как правительству необходимо проанализировать ответы граждан, что будет ошибкой во время кризисных ситуаций, когда счет идет на минуты.

Для наибольшей эффективности нужно создавать платформы для обучения цифровой грамотности или призывать людей к её обучению, как например, это сделала Рабочая группа по безопасности и технологиям в Интернете, призвав обучать цифровой безопасности в частном и правительственном секторах с раннего возраста [10]. Использование вышеперечисленных инструментов мобилизует силы и позволяет каждому из акторов участвовать в диалоге для выработки эффективных решений.

Лоббирование помогает услышать разные голоса в процессе принятия решений, которые необходимы в сложную эпоху цифровизации и борьбы с угрозами. Однако резкое увеличение ИКТ и ускорение развития эпохи цифровизации, вызванное пандемией COVID-19, изменили многое. Лоббирование все ещё развивается умеренными темпами, несмотря на все толчки лоббистских организаций, выражающиеся в увеличении расходов на лоббирование. Улучшаются технологии киберпреступников, проводятся масштабные кибератаки – все это должно мобилизовать деятельность правительств и лоббистских организаций, которым необходимо перестать добиваться победы своей стороны и прийти к общему консенсусу по выработке эффективных правил, законопроектов, направленных на обеспечение цифровой безопасности как своих пользователей, так и граждан в целом. К тому же, такие договоренности смогут привести к более продуктивному диалогу между экспертами технологических компаний, которые будут стремиться помочь правительственным органам при условии, что их интересы будут приниматься во внимание правительством. Необходимо всем сторонам использовать все свои силы, чтобы преодолеть трудности киберпространства, а когда ситуация в мире стабилизируется, то все усилия организаций и властных структур найдут своё эффективное применение в обычных условиях жизни. Намеченная тенденция по развитию краудсорсинговых платформ не должна ускользать от внимания, ведь это возможность услышать граждан для принятия решений на законодательном уровне, которые будут удобны для использования каждым.

Литература:

1. Борцов, М. Ю. Краудсорсинг как инновация для реализации проектов по развитию городской среды: бак. раб. ...студент: 27.03.05 / М. Ю. Борцов. – Томск, 2018. – 79 л.
2. Демченко, К. С. Проблемы взаимодействия власти и бизнеса в условиях цифровизации экономики / К. С. Демченко, О. И. Савва, О. Н. Момотова // Материалы VII ежегодной научно-практической конференции

преподавателей, студентов и молодых ученых Северо-Кавказского федерального университета / под ред. Л. И. Ушвицкого, А. В. Савцовой, 2019. – С. 280–283.

3. Децентрализованные органы и учреждения в системе исполнительной власти зарубежных государств : научно-практическое пособие / Н. М. Касаткина [и др.] ; отв. ред. А. Н. Пилипенко. – М. : ИЗиСП ; Норма ; ИНФРАМ, 2018. – 208 с.

4. Плотникова, Д. Е. Использование digital-инструментов в лоббировании (GR-сопровождении) проектов экологического профиля / Д. Е. Плотникова // Вестник науки и образования. – 2019. – № 10. – С. 54–57.

5. Amazon wages secret war on Americans' privacy, documents show [Electronic resource] // A Reuters Special Report. – Mode of access: <https://www.reuters.com/investigates/special-report/amazon-privacy-lobbying/>. – Date of access: 10.02.2022.

6. Atikcan, E. Ö. Choosing lobbying sides: the General Data Protection Regulation of the European Union / E. Ö. Atikcan, A. W. Chalmers // Journal of Public Policy. – 2019. – № 4. – P. 543–564.

7. Government, private sector need to work together to advance tech innovation and enhance security [Electronic resource] // CNBC. – Mode of access: <https://www.cnbc.com/2022/01/19/government-private-sector-must-work-together-for-advanced-security.html>. – Date of access: 15.02.2022.

8. Council to Secure the Digital Economy [Electronic resource] // CSDE. – Mode of access: <https://csde.org/>. – Date of access: 04.02.2022.

9. 2021 records 'all-time peak' in weekly cyber attacks [Electronic resource] // CYBERSecurityHub. – Mode of access: <https://www.cshub.com/attacks/news/2021-records-all-time-peak-in-weekly-cyber-attacks>. – Date of access: 14.02.2022.

10. Youth Safety on a Living Internet: Report of the Online Safety and Technology Working Group [Electronic resource] // OSTWG Final Report. – Mode of access: https://www.ntia.doc.gov/legacy/reports/2010/OSTWG_Final_Report_060410.pdf. – Date of access: 13.02.2022.

11. Konzerne streichen Milliarden Corona-Gewinne ein [Electronic resource] // Spiegel Wirtschaft. – Mode of access: <https://www.spiegel.de/wirtschaft/corona-pandemie-konzerne-streichen-milliardengewinne-ein-a-1f8d4e23-e3b5-419d-9b89-e8813982be1c>. – Date of access: 02.02.2022.

12. Cybersecurity and national security. Update on Amazon privacy lobbying [Electronic resource] // TheCyberWire. More Signal. Less Noise. – Mode of access: <https://thecyberwire.com/newsletters/policy-briefing/3/225>. – Date of access: 03.02.2022.