Секция «Современная политика в условиях цифровых трансформаций и развития технологий искусственного интеллекта.»

Роль частных компаний в обеспечении национальной кибербезопасности США

Научный руководитель – Морозов Евгений Михайлович

Серова А.С.[1], *Гарифуллин Э.Г.*[2]

1 - Национальный исследовательский ядерный университет «МИФИ», Институт промышленных и ядерных технологий, Москва, Россия, *E-mail: as.serova@mail.ru*; 2 - Национальный исследовательский ядерный университет «МИФИ», Москва, Россия, *E-mail: as.serova@mail.ru*

Стремительное развитие технологий в течение последних десятилетий привело к широкомасштабному процессу цифровизации, затронувшему абсолютно все сферы нашей жизни. Киберпространство стало новой перспективной областью человеческой деятельности. С появлением первых вредоносных программ и началом роста числа и видов кибератак именно частные компании в первую очередь занялись разработкой и развитием способов противодействия. Признавая отсутствие госконтроля за большей частью объектов критической инфраструктуры, связанных с информационными технологиями, правительство Соединенных Штатов Америки вынуждено идти на сотрудничество и партнерство с частным сектором в целях обеспечения национальной кибербезопасности.

Ключевым фактором, сделавшим необходимой государственно-частную кооперацию в информационном пространстве, стало отсутствие прямого контроля и отслеживания правительством США всей инфраструктуры частного сектора в стране. Подобные мероприятия являются технически сложными в связи с исторически сложившейся децентрализацией, основанной на принципах рыночной экономики и институте частной собственности. Каждая компания самостоятельно защищает собственные сети от вторжения и кибератак любого рода за счет привлечения квалифицированных кадров и передовых технологий.

Наиболее значимыми партнерами при противодействии киберугрозам являются крупнейшие IT корпорации, такие как Microsoft, Apple, Google, Facebook и Amazon. Они поставляют свои услуги и оборудование по всему миру. Обеспечение безопасности платформ и сервисов является приоритетной задачей. В свою очередь, интернет-провайдеры развивают безопасность своих сетей и препятствуют распространению через них вредоносных программ.

Существует несколько конкретных механизмов, при помощи которых правительство США осуществляет взаимодействие с частным сектором. Согласно директиве PDD-63 - Critical Infrastructure Protection, подписанной президентом Клинтоном в 1998 году, был создан Центр Обмена Информацией и Анализа (Information Sharing and Analysis Center, ISAC). Он стал платформой для двустороннего обмена информацией между частным сектором и правительством, а также реализует сбор данных об угрозах кибербезопасности критической инфраструктуры[n1]. В основу центра входят отраслевые консорциумы для каждого сектора экономики. Наиболее крупные из них носят международный характер, например, Центр анализа и обмена информацией между финансовыми службами (Financial Services Information Sharing and Analysis Center, FS-ISAC), в состав которого входят представители более 70 стран.

В рамках программы ESF (Enduring Security Framework) проводятся встречи, где представители разведки США предоставляют руководителям и операторам компаний, отнесенных к объектам критической инфраструктуры, информацию о новейших угрозах в киберпространстве, производится совместная выработка механизмов по противодействию

им. В соответствии с целями Национального плана по защите инфраструктуры, принятого Министерством внутренней безопасности США в 2013 году, был создан Консультативный совет по партнерству в области критической инфраструктуры (Critical Infrastructure Partnership Advisory Council, CIPAC). С его помощью реализуется взаимодействие между государственными регуляторами и частными компаниями в целях повышения безопасности стратегических объектов.

Стоит отметить, что инициатива в данной области исходит не только от органов государственной власти. Ярким примером является Программа защиты демократии, запущенная Microsoft в 2018 году. Она была создана для предупреждения избирательных кампаний от взлома, повышения прозрачности политической рекламы в Интернете, поиска технологических решений для поддержания сохранности избирательных процессов, а также защиты от дезинформации [n2]. В рамках проекта компанией было разработано программное обеспечение «Video Authenticator» для борьбы с дипфейками. Данный феномен представляет собой генерируемые нейросетью аудио-видеотехнические материалы трудноотличимые от оригинала. Программа способна в реальном времени рассчитывать процентную вероятность подлинности, покадрово обрабатывая файлы и определяя границу наложения дипфейка. Другая анонсированная технология создана для распознавания деструктивного контента манипулятивного характера. Она состоит из считывателя и инструментов облачного сервиса Microsoft Azure. Концепция разработана Microsoft Research и Microsoft Azure в партнерстве с Программой защиты демократии. В ходе опытной эксплуатации программного обеспечения компанией было проведено статистическое исследование, на основании которого было выявлено 96 политических кампаний, проводимых в социальных сетях, в которых обнаружено иностранное влияние в период с 2013 по 2019 гг. В рамках анализа данных о выборах из 30 стран, было определено, что 93% кампаний основаны на оригинальном контенте, в 86% содержатся дополнения к имеющемуся контенту, а 74% использовали искаженные общеизвестные факты. В связи с пандемией COVID-19 программа использовалась для исследования корректности информации о заболевании. Результаты показали большое количество искаженных данных о методах и средствах лечения, которые способствовали повышению риска госпитализации людей[n3].

Подведя итоги вышесказанного, можно с уверенностью сказать, что на сегодняшний день в США существует хорошо отлаженная система по противодействию киберугрозам, основанная на взаимном сотрудничестве Государственных органов управления и частных IT-компаний. Для полного обзора авторами данной статьи были рассмотрены конкретные примеры частных организаций и государственных компаний, вносящих весомый вклад в решение проблемы угроз киберпространству. Также хочется подчеркнуть, что ввиду стремительного прогресса компьютерной сферы не стоит останавливаться на достигнутом, необходимо развивать и улучшать существующие методы борьбы с кибератаками в качестве превентивной меры перед новыми цифровыми угрозами.

Источники и литература

1) clinton.presidentiallibraries.us (Clinton Digital Library)
2) news.microsoft.com (Новости и истории Microsoft)
3) azure.microsoft.com (Microsoft Azure)