Дляверова Виктория

Студентка 4 курса Наманганского

Инженерно-технологического института.

Проблемы и угрозы цифровизации

Аннотация. Цифровая трансформация неизбежно охватывает всё новые сферы деятельности. Та скорость с которой происходит эта трансформации в жизни общества позволяет называть нынешнюю ступень развития цифровых технологий «цифровой революцией». Практически всё вокруг, включая нас самих, является объектом цифровой трансформации , хотя за видными на первый взгляд возможностями скрываются основательные угрозы, которые необходимо спрогнозировать и осветить в целях предупреждения вероятных отрицательных последствий. Самыми актуальными являются реальные угрозы, которые проявляются на современном этапе технического развития и остро требуют юридических решений. В целом все реальные угрозы связаны с проблемами безопасности личности, бизнеса, общества и государства в цифровой среде.

Ключевые слова : цифровизация, цифровая трансформация , угрозы цифровизации, проблемы цифровизации, риски цифровизации , киберпреступность , кибербезопасность

В процессе внедрения цифровизации развивающиеся страны выделили ряд немало важных проблем связанных с этим процессом. Однако, прежде чем оценивать возможные опасности цифровой трансформации общественных отношений и разрабатывать их решение, нужно определить эти нежелательные последствия, или проблемы цифровизации.

Под цифровизацией в узком смысле понимается преобразование информации в цифровую форму, которое в большинстве случаев ведет к

снижению издержек, появлению новых возможностей и т. д. Большое число конкретных преобразований информации в цифровую форму приводит к таким существенным положительным последствиям, которые обусловливают применение термина цифровизации в широком смысле [1] . Под цифровизацией в широком смысле рассматривается современный общемировой тренд развития экономики и общества, стимулирует ее эффективное развитие экономики, улучшает качество жизни населения [2]. Преимуществами применения цифровой экономики являются снижение стоимости предоставления услуг, развитие электронной коммерции, стимулирование притока иностранного капитала. По оценкам международных экспертов, если развивающиеся страны достигнут уровня проникновения интернета, как у развитых рынков, их долгосрочная производительность увеличится на 25 процентов.

Не смотря на наличие столь весомых положительных последствий внушительный объем проблем цифровизации эксперты связывают с появлением и распространением искусственного интеллекта и как итог с вероятным противостоянием человека и ИИ. Разумно разделить все потенциальные угрозы цифровизации на гипотетические, т.е. возможные в перспективе на высоком уровне технологического развития (уровне прогнозируемом, но в настоящий момент недоступном), и реальные , т.е. очевидные и констатируемые в современном обществе на имеющемся уровне технологического развития.

Гипотетические угрозы связаны, прежде всего, с потенциально возможным появлением сильного ИИ, обладающего автономностью и сопоставимого с интеллектом человека. К гипотетическим угрозам относятся, в частности, возможное противостояние ИИ и человечества, конфликт ИИ с ноосферой, порождающие, в свою очередь, различные угрозы для

существования человечества [3] Большая часть прогнозируемых на сегодняшний день угроз в сфере ИИ касается этических вопросов, точнее, возможных конфликтов современной антропоцентричной морали и логики функционирования будущих автономных носителей сильного ИИ. Исследователи констатируют, что «… развитие тех или иных опасных технологий без учета вопросов этики может привести человечество к совершенно катастрофическому результату» [4].

К *реальным* угрозам цифровизации, которые в полной мере осознаются и являются актуальным уже сегодня, относятся незащищенность персональных данных в киберпространстве и связанная с этим неспособность современных правовых средств осуществить регулирование и защиту общественных отношений; изменение рынка труда и технологическая безработица; распространение киберпреступности и неспособность правоохранительных органов обеспечить безопасность личности в интернет-пространстве; отсутствие правового регулирования Интернета и механизмов действенного государственно-правового контроля в интернет-среде и т.д.

По последним данным объем мирового рынка киберпреступлений составляет 1,5 трлн долл. США. Эта цифра сопоставима с ВВП Канады или Австралии в 2017 г., согласно данным World Bank. Ровно в такую же сумму США оценивает план по восстановлению инфраструктуры своей страны. По некоторым данным, индивидуальные киберпреступники могут зарабатывать в год до полумиллиона долларов США просто торгуя украденными данными.[5]



Рисунок 1. Мировой рынок киберпреступлений

Источник данных: Bromium — разработчик виртуального аппаратного обеспечения в области ИБ

Наибольшее количество кибератак было совершено с территории Узбекистана, Российской Федерации, Германии .

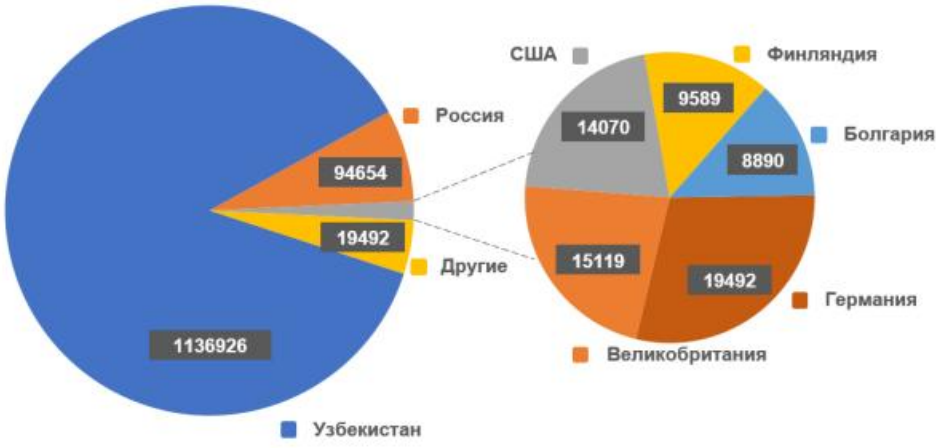


Рисунок 2. Страны с адресного пространства которых осуществлялись кибератаки.

Переходя в частности к Узбекистану , по итогам мониторинга инцидентов кибербезопасности, совершенных в отношении веб-сайтов доменной зоны «UZ», зафиксировано 444 инцидента, из которых наибольшее

количество приходится на несанкционированную загрузку контента (НЗК) – 341 и несанкционированное изменение главной страницы (Deface) – 89 . Анализ инцидентов показал, что веб-сайты государственного сектора (134 инцидент) подвержены атакам в 3 раза реже, по сравнению с частным сектором (310 инцидент).[6]

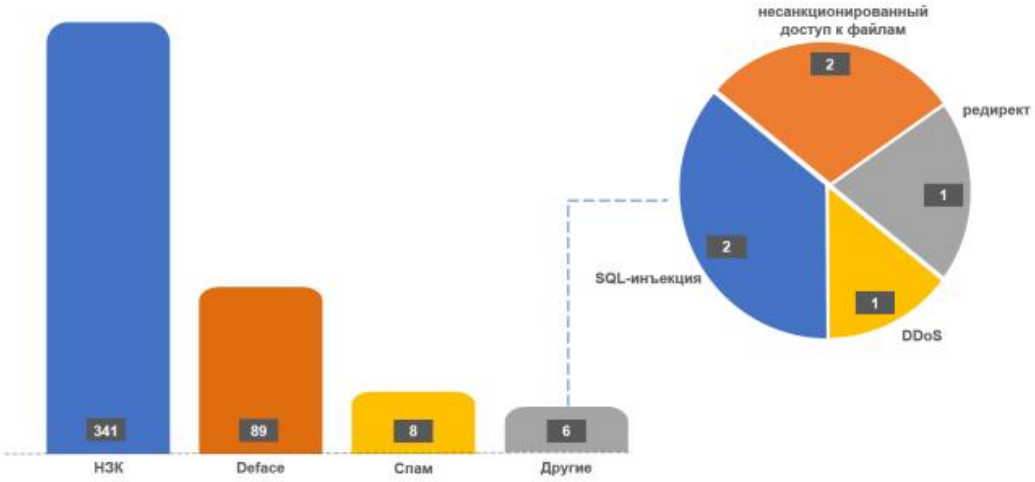


Рисунок 3 . Инциденты кибербезопасности веб-сайтов

Подводя итоги, можно сказать, что основной проблемой цифровизации на сегодняшний день является обеспечение безопасности личности, бизнеса, общества и государства в цифровую эпоху. Проблема безопасности в условиях развития информационных технологий имеет множество проявлений, выступающих в качестве угроз либо отдельным социальным институтам, либо защищаемым законом правам и интересам лиц. По мнению исследователей, решение проблемы возможно только через активную деятельность государства. Именно государство должно создавать определенные правила и регулировать рынок [3]

Список использованной литературы :

1) Сологубова Г. С. Составляющие цифровой трансформации: монография/ Г. С. Сологубова. - Москва: Издательство Юрайт, 2019. 147 с. - (Серия: Актуальные монографии). - ISBN 978-5-534-11335-8. URL: https://biblio-online.ru/book/sostavlyayuschie-cifrovoytransformacii-445006.

2) под ред. А.В. Генераловой. – М.: ФГБОУ ВО «РГУ им. А.Н. Косыгина», 2020. С. 18-22. 3. Халин Г.В. Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы, угрозы и риски/ Г.В. Халин, В.Г. Чернова // Власть и экономика. 2018. № 10. С. 45-64. DOI https://doi.org/10.22394/1726-1139-2018-10-46-63.

3) Самсонова А. Российский IoT не справляется с киберугрозами [Электронный ресурс] // COMNEWS: новости цифровой трансформации, телекоммуникаций, вещания и ИТ. — URL: https://www.comnews.ru/content/204931/2020-03-10/2020-w11/rossiyskiy-iot-ne-spravlyaetsyakiberugrozami?utm_source=telegram&utm_medium=general&utm_campaign=general (дата обращения: 31.03.2020).

4) Ройзензон Г.В. Проблемы формализации понятия этики в искусственном интеллекте [Электронный ресурс] // Шестнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2018. Труды конференции: в 2 томах. — М.: Издательство: Федеральное государственное предприятие «Информационное телеграфное агентство России (ИТАР-ТАСС)» филиал «Российская книжная палата», 2018. — С. 245–252. — URL: https://elibrary.ru/item.asp?id=35568660 (дата обращения: 25.09.2019).

5) https://www.aktiv-company.ru/analitics/articles/cybercryme.html

6) https://tace.uz/ru/news/kiberbezopasnost-respubliki-uzbekistan-itogi-2021-goda/