Хосиев Вахид (Казахстан)

Томский политехнический университет г. Томск

Научные руководители: Макиенко Марина Алексеевна, доцент ТПУ,
Садовская Анна Александровна

# ПРОБЛЕМА КИБЕРБЕЗОПАСНОСТИ В КОНТЕКСТЕ РАЗВИТИЯ СМАРТ-ТЕХНОЛОГИЙ

Исследование выполнено за счет гранта Российского научного фонда (проект РНФ № 22-28-00061) «Смарт-технологии как фактор социальной политики и терминологического планирования: социолингвистический подход», https://rscf.ru/project/22-28-00061/

В современном мире необходимо говорить не об отдельно взятой технологии, а о комплексе, взаимодействии смарт-технологий посредством Интернета вещей (IoT). Концепция интернета вещей представляется достаточно простой и очевидной в контексте развития системы Интернет: объединение различных вещей, предметов, программ как реальных, так и виртуальных (например, электронная библиотека или образовательный контент) в единую открытую систему. По данным компании Strategy Analytics в 2018 году общее количество устройств во всем мире, подключенных к Интернету вещей достигло 22 млрд. Прогнозируется, что к 2030 году количество таких устройств достигнет 50 млрд. Конечно, это не единственный прогноз. Для сравнения, Juniper Research прогнозирует, что количество в 50 млрд. устройств будет уже в 2022 году [1]. Такое увеличение объясняется тем, что Интернет вещей объединяет ключевые направления, по которым происходит развитие смарт-технологий: смарт-транспорт, смарт-образование, смарт-медицину, смарт-промышленность, смарт-энергию, смарт-город, смарт-хозяйство (сельскохозяйственный комплекс).

Важно отметить, что Интернет вещей преобразует повседневную жизнь человека, создавая специфические требования к системе ценностей: взаимная ответственность в контексте заботы о кибербезопасности используемых устройств; доверие и открытость. Тема кибербезопасности является чрезвычайно актуальной, поскольку речь идет не только о личных данных и личной безопасности индивида, но и о безопасности больших групп населения в результате взлома банков, предприятий, систем энергообеспечения и т.д.

Можно выделить несколько укрупненных направлений, по которым осуществляется разработка вопроса кибербезопасности:

Формирование киберполитики в рамках государства. Здесь исследователи выделяют межнациональное и межсекторальное направление, а также формирование законодательства в области обеспечение безопасности физических лиц [2]. В качестве примера можно привести 74 сессию Генассамблеи ООН, на которой Россия представила проект резолюции о противодействии использованию информационно-коммуникационных технологий в преступных целях. На данный момент в мире отсутствует единое правовое поле для борьбы с киберпреступлениями, государства чаще заключают двусторонние соглашения [3]. В этом контексте необходимо отметить, что в июле 2021 года Президентовм РФ был подписан Указ «О Стратегии национальной безопасности Российской Федерации» [4]. В стратегии выделены основные информационные угрозы, основные направления обеспечения информационной безопасности, а также мероприятия, нацеленные на реализацию указанных направлений. Необходимо также отметить, что регулярно проводятся международные конференции по кибрбезопасности. В качестве примера можно привести состоявшийся в 2021 году международный ежегодный онлайнтренинг по кибербезопасности Cyber Polygon [5], международный форум «Интерполитех: цифровая трансформация безопасности государства» [6] и т.д.

Формирование киберполитики в рамках отдельного предприятия. Данное направление охватывает различные сферы: деятельность финансовых организаций, деятельность организаций, использующих Интернет вещей. Кибербезопасность финансовых организаций определяется вопросами утечки личных данных клиентов, например, данных кредитных или банковских карт, персональных данных, кибератаки на криптосервисы, фешинговые письма. В области Интернета вещей вопросы кибербезопасности затрагивают аспекты информации, передающейся между различными составляющими Интернета вещей, на основании которой происходит принятие решений, обработки больших массивов данных, их хранения в облачных системах, взаимодействия VR, AR и физической реальности. В конечном счете, деятельность предприятия и конечного пользователя продукции зависит от работы систем кибербезопасности [7].

Формирование личной ответственности человека за индивидуальную кибербезопасность. В этом контексте речь часто идет о социальных технологиях, которые могут быть использованы и в негативном варианте (как мера воздействия на человека при кибератаках), так и в позитивном варианте (как осознание человеком личной ответственности за собственную кибербезопасноть) [8].

В контексте указанной выше проблемы кибербезопасности, актуализируется тема доверия в современном обществе в контексте развития

Интернета вещей. Впервые эта тема прозвучала у лауреата Нобелевской премии по экономике 2009 года, Элионор Остром (Elinor Ostrom) Она предлагает идею полицентричного управления, основанного на доверии властей группам. Результатом чего, будет разумная организация людьми пространства для жизни. Проанализировав существующие на данный момент модели в сфере экономической политики – концепцию «Трагедии общин» Хардина, концепцию «диллема заключенного» и концепцию логики коллективного действия М. Олсона, она приходит к выводу о том, что основанные на данных моделях методы принятия решений в рамках экономической политики не могут быть единственными. Вариант экономической модели, развиваемый тремя указанными концепциями, при которой люди в любом случае не будут сотрудничать, не может быть однозначным. Э. Остром указывает на то, что необходимо выделить переменные, которые повлияют на возможность местного небольшого сообщества самостоятельно организоваться, имея ввиду основания для взаимодействия групп людей, интересы которых противоположны. В том случае, если эти группы людей живут на ограниченной территории, вынуждены постоянно взаимодействовать друг с другом, то они с высокой степенью вероятности будут искать, кому можно доверять, будут осознавать последствия деятельности для социума и природы, образуя таким образом, социальный капитал. Но необходимо отметить, что это только одно правило для организации позитивного взаимодействия. Помимо этого, выделены также следующие составляющие: изменение правил функционирования в контексте достижения единой цели – общее благосостояние, понимание того, что группа присваивателей потерпит ущерб, если не примет общие правила взаимодействия. Необходимо еще раз акцентировать внимание, что автор говорит о небольших, устойчивых группах людей, поэтому, данные принципы могут быть применены только к устойчивой, небольшой группе людей. Но часто современные смарт-города – это как раз относительно устойчивые, небольшие города, либо устойчивые, небольшие сообщества в рамках крупных городов [9].

Необходимо отметить, что сопутствующей системой для развития различных видов смарт-технологий будет развитие кибербезопасности как необходимой составляющей абсолютно всех технологий с использованием Искусственного интеллекта. Данный аспект также необходимо учесть в категории «умные технологии» - антивирус «улавливает» вирус (компьютерный в данном случае) без участия пользователя, определяя его по некоторым свойствам.

Представленная выше проблематизация темы кибербезопасности в контексте развития смарт-технологий, актуализирует вопрос оснований для реализации данного концепта в повседневной жизни и конечного

пользователя, и изобретателя, и конкретного предприятия, и государства. На наш взгляд осмысление основ формирования кибербезопасности должно происходить в следующих плоскостях: технической, экономической, социальной, законодательной.

## СПИСОК ЛИТЕРАТУРЫ


1. Juniper Research [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9,_IoT,_M2M_(%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%BE%D0%B9_%D1%80%D1%8B%D0%BD%D0%BE%D0%BA (дата обращения: 12.03.2022)
2. Ido Sivan-Sevilla Framing and governing cyber risks: comparative analysis of U.S. Federal policies [1996–2018] // Journal of Risk Research https://doi.org/10.1080/13669877.2019.1673797
3. Официальный сайт ТАСС [Электронный ресурс]. – Режим доступа: https://tass.ru/politika/7005096 (Дата обращения: 07.03.2022)
4. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_389271/ (Дата обращения: 28.02.2022)
5. Официальный сайт международного полигона по наращиванию киберустойчивости Cyber Polygon [Электронный ресурс]. – Режим доступа: https://cyberpolygon.com/ (Дата обращения: 28.02.2022)
6. Официальный сайт Второго Международного форума «Интерполитех: цифровая трансформация безопасности государства» [Электронный ресурс]. – Режим доступа: https://www.interpolitex.ru/forum/ (Дата обращения: 20.03.2022)
7. (Yang H., S. Kumara The Internet of things for Smart manufacturing: a review // IISE Transactions. Volume 51, 2019. – Issue 11. https://doi.org/10.1080/24725854.2018.1555383
8. Lena Y. Conolly, David S. Wall The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures // Computers Security. – Volume 87.- November 2019. 101568.
9. Остром Э. Управляя общим. Эволюция институтов коллективной деятельности. – М.: Мысль, ИРИСЭН, 2011. – 447 с.