ИССЛЕДОВАНИЕ ПУТЕЙ РАЗВИТИЯ ПРОМЫШЛЕННОЙ ИНТЕРНЕТ-БЕЗОПАСНОСТИ В УСЛОВИЯХ ЭКОНОМИЧЕСКОЙ ГЛОБАЛИЗАЦИИ

Сюе Цяньвэнь

аспирантка Белорусского государственного университета
Научный руководитель – Г.Г. Головенчик, кандидат экономических наук, доцент

Являясь продуктом глубокой интеграции нового поколения цифровых технологий и производственных процессов, промышленный интернет вещей становится не только важным фактором реиндустриализации развитых стран, но и предоставляет развивающимся странам возможность осуществить трансформацию и модернизацию обрабатывающей промышленности. В статье проанализированы тенденции развития промышленного Интернета, выявлены связанные с ним проблемы, внесены предложения по развитию промышленного Интернета.

***Ключевые слова*:** промышленный интернет вещей; цифровизация; глобализация; безопасность.

В последние годы мировая экономика демонстрирует две основные тенденции развития. Во-первых, после серьезного сокращения объемов традиционной промышленности развитые страны пытаются оживить реальную экономику за счет создания передового высокоинтеллектуального производства. Во-вторых, развивающиеся страны постепенно утрачивают свои преимущества в стоимости рабочей силы и других факторов производства, все более заметными становятся местные экологические проблемы, а первоначальная модель экстенсивного развития становится всё более неустойчивой. В контексте четвертой промышленной революции, фундаментом которой являются цифровые технологии, во всем мире сложился консенсус в отношении содействия трансформации и модернизации традиционных отраслей путем глубокой интеграции цифровой и реальной экономики, и придания на ее основе нового импульса экономическому развитию. Являясь продуктом глубокой интеграции нового поколения цифровых технологий и производственных процессов, промышленный интернет вещей (Industrial Internet of Things, IIoT) стал важной опорой Индустрии 4.0. Хотя эта новая концепция обеспечила рациональное использование ресурсов, снижение производственных затрат и повышение эффективности производства, ее быстрое внедрение также расширило возможность атак «умного» производственного оборудования и глобальных цепочек создания добавленной стоимости, что принесло новые риски для безопасности промышленных объектов. Эффективное предотвращение и устранение нарушений в системах безопасности, возникающих в результате использования промышленного интернета, стало актуальной проблемой для множества стран.

Во втором десятилетии XX в. основные промышленные страны мира приняли IIoT в качестве носителя интеллектуальной трансформации традиционных отраслей и ввели соответствующую политику, чтобы помочь развитию промышленного интернета вещей в своих странах. В 2011 г. США выпустил «Программу

партнерства в области перспективного производства», а затем, в 2012 г. General Electric предложил концепцию промышленного Интернета в своем отчете «Промышленный Интернет: разрыв границы между мудростью и машиной». В 2013 г. Германия опубликовала «Стратегию Индустрии 4.0». В 2015 г. Китай выпустил «Сделано в Китае 2025». в 2017 г. Япония предложила «подключенную индустрию». Хотя эти политики и меры различны, все они подчеркивают возможности, которые новое поколение информационных технологий открывает для традиционных отраслей.

Будучи неизбежным следствием цифровизации и глобализации, IIoT включает тесно связанные между собой интеллектуальные устройства, оснащенные встроенными технологиями сбора и передачи информации, промышленные интернет-платформы, соединяющие их компьютерные сети, инструменты хранения и анализа данных, а также обслуживающий всё это высококвалифицированный персонал [1]. С помощью нового поколения цифровых технологий IIoT тесно связывает представителей различных фирм со всего мира, способствует цифровой трансформации бизнес-процессов в области проектирования, закупки, производства, складирования, маркетинга, транспортировки, продаж и послепродажного обслуживания, позволяет компаниям преодолеть барьеры физического пространства в рамках традиционной модели промышленного производства, беспрепятственно обмениваться информацией в режиме реального времени и продуктивно сотрудничать на больших расстояниях, в конечном итоге содействует повышению качества продукции и эффективности работы предприятий.

Промышленный интернет помогает предприятиям внедрять в производственный процесс роботов и системы автоматизации, повышать качество профилактического технического обслуживания и выявлять дефекты оборудования до того, как они повлияют на качество выпускаемой продукции.

В 2020 г. IIoT быстро развивался в основных индустриальных странах мира, среди которых наиболее выдающиеся результаты показали США, Германия, Япония и Китай. Добавленная стоимость промышленного интернета в вышеуказанных четырех странах составляет 885,84 млрд долл., 247,594 млрд долл., 305,566 млрд долл. и 566,456 млрд долл. США соответственно [2].

Опыт основных индустриальных стран показывает, что IIoT представляет собой новое направление будущего развития мировой индустрии. Но необходимо отметить что, промышленный интернет вещей не только открывает новые возможности для всех стран по осуществлению трансформации и модернизации промышленного производства, но и несет с собой новые риски. Разнообразные и сложные экономические структуры, задействованные в IIoT, расширили зону его атак. В настоящее время во всем мире регистрируется множество инцидентов, связанных с безопасностью IIoT, которые уже серьезно подорвали экономические выгоды предприятий и поставили под угрозу социальную стабильность и национальную безопасность в ряде стран. С точки зрения произошедших инцидентов, вопросы обеспечения безопасности IIoT можно разделить на две большие группы: технические проблемы и проблемы управления.

Технические проблемы включают в себя прерывание поставок технологий IIoT и кибератаки на объекты критической инфраструктуры и глобальные цепочки создания добавленной стоимости, основанные на IIoT.

Промышленный интернет вещей зародился в США, и до настоящего времени основная масса технологий, способствующих его развитию, разрабатывается в развитых странах, прежде всего, США и Германии. Большинство стран осуществляют цифровую трансформацию промышленности за счет внедрения заимствованных технологий, поэтому прерывание или ограничение их поставок стало потенциальным препятствием для развития IIoT. Например, цифровая трансформация производства в Китае сильно зависит от поставок ряда критических технологий из США. Следствием усиления торговых трений между КНР и США стало введение американских санкций против Китая. По состоянию на начало 2021 г. США включили 484 китайских предприятия в «Список юридических лиц», которым отказано в продаже базовых и ключевых новых технологий. Таким образом, промышленная и экологическая стабильность Китая в определенной степени поставлена под угрозу [3].

В большинстве стран мира имеются информационно-телекоммуникационные сети и системы, управляющие объектами критической инфраструктуры (к ним можно отнести услуги связи, энергетику, транспортные и финансовые услуги, ЖКХ и т.д.), в основе которых лежит IIoT. Такие объекты должны быть надежно защищены от внешних угроз, в том числе от кибератак. Однако в связи с распространением систем промышленного интернета возникают дополнительные уязвимости в системе кибербезопасности, что ставит под угрозу безопасность всей системы в целом и дает возможность злоумышленникам для атаки, последствия которой могут быть катастрофическими: изменение температуры в системах охлаждения атомных реакторов, отключение питания в больницах и т.д. Кроме того, IIoT соединяет промышленные предприятия по всему миру с помощью таких технологий, как искусственный интеллект, большие данные и интернет вещей, и способствует цифровизации и глобализации цепочек создания добавленной стоимости в традиционной промышленной сфере. В этом контексте значительно возрастает возможность атаки промышленных предприятий, а вторжение в информационную систему одного объекта наносит существенный ущерб предприятиям во всей цепочке и даже подрывает национальные интересы.

По данным «Лаборатории Касперского», в России 45% компаний уже используют технологии IIoT, при этом 31% из них столкнулись в 2019 г. с атаками на подключённые устройства. Статистика «Лаборатории Касперского» показывает, что за 2015-2020 гг. количество новых образцов вредоносного ПО для промышленного интернета вещей выросло почти в 700 раз – с 483 до 331401 [4]. Эксперты Positive Technologies проанализировали киберугрозы 2020 г. и выяснили, что по сравнению с 2019 г. количество инцидентов на промышленных предприятиях увеличилось на 91%, а число атак с использованием malware возросло на 54%. Интересно, что семь из десяти атак носили целенаправленный ха-

рактер: операторы вымогателей стали тщательней выбирать цели – изучая финансовое положение компаний на рынке, оценивая значимость отрасли и потенциальные последствия атаки для компании-жертвы. Больше всего злоумышленников интересовали государственные учреждения (19%), промышленные компании (12%) и медицинские организации (9%). По сравнению с прошлым годом, в 2020 г. число атак на промышленные компании выросло почти вдвое: прирост составил 91%. В основном эту отрасль атаковали операторы программ-вымогателей, в частности RansomExx, Netwalker, Clop, Maze, Ragnar Locker, LockBit, DoppelPaymer, а также Snake, который перед началом шифрования удаляет теневые копии и имеет функции, позволяющие принудительно остановить процессы в АСУ ТП [5].

Согласно отчету Китайской академии информационных и коммуникационных технологий, в первой половине 2020 г. в Китае было совершено 13,56 млн злонамеренных кибератак, которые затронули 2039 компаний [6].

Другая группа проблем заключается в неэффективном управлении предприятиями, что также ведет к возникновению угроз безопасности систем промышленного интернета. Цифровизация отражается на всех стадиях производственного цикла, таких как закупка сырья и материалов, доставка товара к потребителю, его использование и послепродажное обслуживание. В этот процесс включено множество экономических субъектов, таких как поставщики, производители, посредники, потребители и т.п. Когда одно из звеньев не имеет надежных инструментов обнаружения и оценки потенциальных угроз и отлаженной системы управления кибербезопасностью, подвергается атаке, другие компании в цепочке поставок также будут повреждены [7].

С учетом проблем, возникающих при развитии IIoT, выдвинем следующие предложения:

– необходимо ускорить разработку отечественных базовых технологий IIoT. Использование разработанных за пределами страны технологий может решить проблему нехватки технологий в краткосрочной перспективе, но долгосрочная технологическая зависимость не способствует инновационному развитию страны. В связи с этим следует укреплять систему фундаментальных исследований и преодолевать технические трудности, основываясь на достижениях отечественной промышленности;

– требуется усилить подготовку профессиональных кадров в области IIoT. Развитие IIoT выдвинуло более высокие требования к качеству специалистов, которые также должны обладать профессиональными знаниями в области промышленного производства. Можно поощрять высшие учебные заведения к подготовке специалистов в сфере искусственного интеллекта и больших данных путем предоставления льгот в области налогообложения и жилищного строительства;

– рекомендуется выстроить технологическую систему кибербезопасности в области IIoT. Создать механизм обнаружения, оценки и предотвращения рисков и управления чрезвычайными ситуациями при возникновении потенциальных

угроз системе IIoT, а также укрепить возможности компании в области защиты промышленного оборудования;

– необходимо укреплять международное сотрудничество в области обеспечения промышленной безопасности, поскольку в условиях глобализации промышленного производства любое упущение в каком-либо звене может негативно повлиять на все предприятия, включенные в цепочку поставок; на постоянной основе осуществлять международный обмен в области цифровых технологий, их стандартизации и сертификации, создать комплексную систему безопасности цепочки поставок на базе промышленного интернета вещей.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. *Ван Сяося*. Обзор промышленных интернет-приложений // Цифровая печать. 2021. № 2. С. 1–3.

2. Китайский научно-исследовательский институт промышленного Интернета. Белая книга по экономическому развитию индустрии промышленного Интернета в Китае (2021 г.). 2021. С. 6–7.

3. *Ду Чуаньчжун*. Опыт развития промышленного Интернета вещей в США и его уроки для Китая // Новости зарубежных исследований Тайпин. 2020. № 7. С. 89–93.

4. Треть российских компаний, использующих интернет вещей, столкнулись с кибератаками на него [Электронный ресурс] // Лаборатория Касперского. URL: https://www.kaspersky.ru/about/press-releases/2020_tret-rossiiskih-kompanii-ispolzuyuschih-internet-veschei-stolknulis-s-kiberatakami-na-nego. (дата обращения: 20.10.2021).

5. Актуальные киберугрозы: итоги 2020 года // Positive Technologies [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/. (дата обращения: 20.10.2021).

6. *Хэ Сиксунь, Чжан Юйцин*. Обзор безопасности цепочки поставок программного обеспечения // Журнал информационной безопасности. 2020. № 1. С. 57–61.

7. *Фан Пейру, Ли Цзюнь*. Пути развития безопасности цепочки поставок промышленного Интернета // Китайская инженерная наука. 2021. № 2. С. 57–60.