Сергей Николаевич Тощук
аспирант кафедры информационных технологий и защиты информации
Ростовского государственного экономического университета «РИНХ»,
г. Ростов-на-Дону, toshchuk@yandex.ru

ВЛИЯНИЕ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ ТЕХНОЛОГИЙ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ (IIoT): РИСКИ, ПРОБЛЕМЫ, ПЕРСПЕКТИВЫ, ТЕНДЕНЦИИ РАЗВИТИЯ

Аннотация. В статье рассматриваются особенности влияния промышленного Интернета вещей на экономическую безопасность предприятия. Отдельное внимание уделено проблемам, возникающим в связи с использованием IIoT. На основе методологии оценки рисков ISO/IEC 27005 систематизированы риски, связанные с промышленным Интернетом вещей для экономической безопасности предприятия. Кроме того, обозначены возможности и перспективы, которые открывает цифровизация, а также применение прорывных технологий на базе IIoT для промышленного производства.

Ключевые слова: промышленный Интернет вещей, экономическая безопасность, предприятие, риск, угроза, данные.

Sergey Nikolaevich Toschuk
Postgraduate student, Department of Information Technology and Information Security
Rostov State University of Economics, Rostov-on-Don, toshchuk@yandex.ru

IMPACT ON THE ECONOMIC SECURITY OF THE INDUSTRIAL INTERNET OF THINGS (IIOT): RISKS, PROBLEMS, PROSPECTS, DEVELOPMENT TRENDS

Abstract. The article deals with the peculiarities of the impact of the Industrial Internet of Things on the economic security of the enterprise. Particular attention is paid to the problems arising from the use of IIoT. Based on the ISO/IEC 27005 risk assessment methodology, the risks associated with the Industrial Internet of Things for the economic security of the enterprise are systematized. It also outlines the opportunities and prospects that digitalization and the use of breakthrough technologies based on IIoT for industrial production.

Keywords: Industrial Internet of Things, economic security, enterprise, risk, threat, data.

XXI век несет с собой «сетевую цивилизацию», «Индустрию 4.0» и «цифровую экономику». Как следствие сегодня трудно представить современный бизнес без интернета и мобильной связи, стремительно ворвавшихся не только во всемирное экономическое пространство, но и в обыденную жизнь каждого человека. Современное развитие мировой экономики и общества происходит за счет внедрения ключевых технологий, лежащих в основе промышленного Интернета вещей (IIoT): блокчейна, облачных вычислений, больших данных, киберфизических систем [1]. Их использование приводит к положительным экономическим и социальным эффектам: автоматизации и интенсификации традиционных экономических и технологических процессов, созданию новых отраслей экономики; улучшению делового и инвестиционного климата за счет повышения доступности и эффективности государственных услуг, прозрачности условий ведения бизнеса; повышению для населения доступности, качества и удобства услуг медицины, образования, культуры, финансов; созданию комфортных для жизни безопасных городов.

В данном контексте стремление к занятию лидирующих позиций на рынке подталкивает руководителей предприятий, а также других влиятельных участников экономической системы разрабатывать инновационные подходы к организации бизнес-процессов на базе передовых технологий, прорывных инноваций с целью повышения результативности операционной деятельности и получения сверхприбылей.

Вследствие активизации обозначенных процессов в настоящее время во многих странах мира реализуются государственные программы цифровизации национальных экономик, результаты которых Всемирный экономический форум оценивает в мировом масштабе более чем в 30 трлн США доходов к 2025 г. Если же рассматривать в разрезе стран, то рост экономических систем за счет стоимости, создаваемой цифровыми технологиями, может составить в Китае 22% ВВП, в США — от 1,6 до 2,2 трлн долл. На данный момент времени доходы цифровой экономики равны 22,5% от общего объема мировой экономики [2].

В то же время существуют определенные риски и угрозы, которые цифровизация несет экономике и обществу. По данным анализа Cybersecurity Ventures, к 2023 г. ущерб от киберпреступлений может составить 6 трлн США [3]. В таких условиях очевидно, что активное внедрение цифровых технологий на предприятиях всех отраслей промышленности, в том числе IIoT, вносит изменения в систему выявления, оценки и минимизации рисков и угроз экономической безопасности. Широкое использование промышленного Интернета вещей стимулирует появление новых угроз, которые обусловлены процессами цифровизации экономики и промышленных процессов в частности. Все это в совокупности значительным образом повышает общий уровень угроз экономической безопасности предприятий.

С учетом вышеизложенного, особую значимость на сегодняшний день приобретают вопросы создания системы обеспечения экономической безопасности предприятия, которая будет учитывать возможности и угрозы промышленного IIoT, обеспечивать достаточный уровень его ресурсного потенциала, создавать условия для безопасного экономического развития и повышения уровня конкурентоспособности, способствовать всестороннему решению тактических и стратегических задач, стоящих перед предприятием в условиях цифровой экономики.

Таким образом, обозначенные обстоятельства предопределяют выбор темы данной статьи, а также свидетельствуют о ее теоретической и практической значимости.

Вопросы, связанные с «цифровизацией» современных предприятий, рисками и перспективами использования промышленного Интернета вещей сегодня исследуют специалисты в различных областях научных знаний, из числа наиболее известных следует отметить Е.В. Маркушину, Н.А. Балову, Т.О. Толстых, С.Е. Афонина, Balaji, K.; Selvam, M.; Rajeswari, R.; Liu, Lixin; Li, Wenzhuo; He, Wu. Отдельные направления обеспечения экономической безопасности предприятий в условиях цифровизации были исследованы в работах таких ученых как: И.В. Манахова, Е.В. Левченко, А.Х. Евстафьева, Е.Ю. Шкловец, Gul, Ejaz; Chaudhry, Imran Sharif. Особое внимание именно взаимосвязи понятий «экономическая безопасность», «цифровизация» и «Индустрия 4.0» на

макроэкономическом уровне и на уровне конкретных предприятий уделено А.С. Денисовой, С.С. Солдатовой, М.И. Дроздовой, Siegel, Joshua E.; Kumar, Sumeet; Sarma, Sanjay E.

Однако, несмотря на достаточно существенную научную наработку отечественных и зарубежных исследователей в этом направлении в течение последних лет, все еще не до конца изученной остается проблема обеспечения экономической безопасности субъектов предпринимательства в условиях внедрения передовых решений цифровой экономики. В частности, открытыми остаются вопросы определения возможного перечня объектов внедрения промышленного Интернета вещей для промышленных предприятий. Особого внимания заслуживают ключевые аспекты формулирования основных задач системы экономической безопасности предприятия в условиях цифровых трансформаций. В более глубоком исследовании нуждается проблема трансформации угроз цифровизации для промышленных предприятий и интенсификации использования технологий IIoT.

Таким образом, с учетом вышеизложенного, цель статьи заключается в рассмотрении особенностей влияния на экономическую безопасность технологий промышленного интернета вещей (IIoT), с отдельным акцентированием внимания на рисках, проблемах, перспективах и тенденциях его развития.

Итак, прежде всего, отметим, что промышленный интернет вещей (IIoT) — это использование интеллектуальных датчиков и исполнительных механизмов для улучшения производственных и промышленных процессов. IIoT в полной мере реализует возможности умных машин и аналитики в режиме реального времени, чтобы воспользоваться данными, которые оборудование и агрегаты генерируют в обычных промышленных условиях. Философия IIoT заключается в том, что умные машины не только лучше людей собирают и анализируют данные в режиме реального времени, но и лучше передают важную информацию, которая может быть использована для принятия более быстрых и точных бизнес-решений [4].

В свою очередь экономическая безопасность субъекта хозяйствования — это состояние эффективного использования его ресурсов для предотвращения вызовов и угроз, а также обеспечения устойчивого функционирования на рынке.

В зависимости от области применения, использование промышленного Интернета вещей может привести к различным рискам, угрожающим целостному комплексу экономической безопасности предприятия: начиная от утечки важной информации, которая имеет решающее значение для работы всего предприятия в целом, до компрометации производимой продукции или повреждения промышленных систем управления.

С учетом вышеизложенного, представляется целесообразным схематически формализовать взаимосвязь технологий IIoT и экономической безопасности предприятия (рис. 1).

Рассматривая более подробно рисунок 1, можно отметить следующее:

1. С одной стороны, бесспорно, использование технологий IIoT на промышленном предприятии несет с собой определенные угрозы и риски, включая угрозы «кибератак». С другой стороны, угрозы и риски, инициируемые промышленным Интернетом вещей, нивелируются функционированием системы

экономической безопасности предприятия. Концепция безопасности трансформационных преобразований предприятия под влиянием технологий IIoT заключается в том, что происходящие модификации могут считаться безопасными, если существующая система экономической безопасности предприятия может спрогнозировать, заблаговременно идентифицировать и оценить возможные угрозы и негативные тенденции, вызванные этими преобразованиями, обеспечить максимально возможную защиту от их влияния, разработать и оперативно реализовать мероприятия по их предотвращению и ликвидации или нивелированию последствий.

2. С другой стороны, система экономической безопасности может использовать цифровые технологии и возможности, которые раскрывает IIoT, способствующие росту эффективности обеспечения экономической безопасности. Т.е. для эффективной защиты в условиях цифровизации система экономической безопасности предприятия и сама нуждается в новейших технологиях и прорывных инновациях.

Рис. 1. Взаимосвязь технологий IIoT и экономической безопасности предприятия

Источник: составлено автором.

Таким образом, можно выделить следующие проблемы IIoT, которые способны нанести ущерб экономической безопасности предприятия:

– перехват промышленного устройства — это происходит, когда злоумышленник получает контроль над конечным оборудованием или датчиком IIoT, часто без ведома владельца. В результате чего производственная линия может начать выпускать некачественную продукцию, продукцию с браком, которая выйдя на рынок, приведет к значительным потерям со стороны предприятия, ухудшению его имиджа, нарушению партнерских отношений с клиентами, что соответственно отрицательным образом скажется на его прибыльности и рентабельности;

– перехват данных. Подобно атаке типа «подслушивание», перехват данных сосредоточен на информации, передаваемой промышленным IIoT-

устройством, а не конечным пользователем. В этом случае злоумышленники подслушивают сетевой трафик, идущий от конечного устройства обратно в основную сеть, чтобы собрать информацию, к которой они не должны иметь доступа [5]. Эта проблема IIoT наиболее опасна, когда данные, которые отправляет промышленное IIoT-устройство, очень чувствительны или могут стать проблемой, если попадут в чужие руки. Это касается коммерческой тайны, секретных технологий изготовления продукции, что особенно опасно для высокорегулируемых отраслей, таких как оборонно-промышленный комплекс, топливо-энергетический комплекс, здравоохранение и аэрокосмическая промышленность. Соответственно раскрытие конфиденциальной информации грозит предприятию потерей своих преимуществ, нивелированию имеющихся конкурентных возможностей и вообще выходу с рынка;

– распределенная атака типа «отказ в обслуживании» на все устройства или на саму внутреннюю сеть промышленного предприятия. В этом случае злоумышленники могут использовать само устройство или централизованную сеть в качестве входа, а затем переполнить конечные устройства таким количеством трафика, что они не смогут выполнить работу, для которой были предназначены [6]. В результате все производство предприятия останавливается, заказы не выполняются в срок, продукция не отгружается, платежи выходят в статус просрочки. Эта проблема очень важна для предприятий, которые полагаются на работоспособность устройств для продолжения производства;

– утечка данных. Эта проблема схожа с проблемой перехвата данных, однако благодаря уязвимым промышленным устройствам, злоумышленники могут украсть не только информацию о технологиях, производственных цепочках, но и данные о любой сфере деятельности предприятия, например:

1) данные клиента или партнера: любая информация о клиентах или партнерах, включая их пароли, информацию о контрагентах или их внутренних системах;

2) личная информация: это могут быть личные или идентифицирующие данные клиентов или сотрудников предприятия;

3) интеллектуальная собственность или коммерческая тайна: все, что имеет жизненно важное значение для работы предприятия, его клиентов или партнеров, что могло бы нанести вред, убытки, если бы оказалось в руках конкурентов;

4) персональные данные;

5) финансовые данные: информация о финансах предприятия, платежах клиентов, партнеров, включая банковские реквизиты.

Итак, ведущий международный опыт свидетельствует о том, что IIoT позволяет существенным образом упростить производственные процессы, в которых акцент смещается на интеграцию, оцифровку и управление всеми физическими ресурсами посредством единообразного и гибкого подхода. Однако это возможности значительным образом усложняют ситуацию с кибербезопасностью, поскольку потенциальный ущерб, нанесенный производственной среде из-за взлома, может быть очень значительным. Атрибуты безопасности (конфиденциальность, целостность и доступность) представляют способы оценки

и сравнительного анализа данных о безопасности сети [7]. Риски IIoT в европейских государствах анализируются на основе методологии оценки рисков ISO/IEC 27005, которая принимает во внимание следующие параметры: типы угроз, субъекты угроз, основные активы и их уровень чувствительности, уязвимости, риски и связанные с ними ситуации.

В таблице 1 представлена классификация рисков и уровень их воздействия на экономическую безопасность предприятия.

Таблица 1

Классификация рисков IIoT, влияющих на экономическую безопасность предприятия

Классификация рисков	*Нарушение/компрометация службы безопасности*	*Уровень риска*
Злоупотребления (неправомерное использование, изменение, кража, уничтожение информации о целевых системах ИКТ, сети и инфраструктуре)	Конфиденциальность, целостность, доступность	Высокий
Прерывание или получение контроля над коммуникацией третьей стороны без разрешения)	Конфиденциальность	Высокий
Вывод из строя оборудования (случайной, форс-мажорные обстоятельства и т. д.)	Доступность	Выше среднего
Непреднамеренный/случайный ущерб	Целостность	Высокий
Нарушение обслуживания и технического ремонта	Доступность	Высокий
Отказ/неисправность (частичное или полное отсутствие функциональности аппаратных /программных средств)	Доступность	Высокий

Источник: составлено автором.

Перспективы и тенденции развития экономической безопасности предприятий под влиянием IIoT связаны с выделением ее новой составляющей, такой как информационная безопасность. С внедрением в жизнь цифровой экономики информационная безопасность приобретает статус самостоятельного элемента окружения предприятия, поскольку выявление угроз, предотвращение опасностей, разоблачение мошенничества в цифровой среде создает условия для достижения целей финансово-хозяйственной деятельности организации, гарантирует устойчивое развитие предприятия и его экономическую и информационную безопасность, что имеет первостепенное значение в условиях цифровой экономики.

Реализоваться новый формат экономической безопасности, дополненный информационной составляющей, может с помощью таких технологий IIoT, как аналитические инструменты, искусственный интеллект и машинное обучение, цифровые двойники, дополненная реальность.

Таким образом, подводя итоги, отметим, что промышленный Интернет вещей позволяет повысить уровень производства инновационной продукции,

обеспечить соответствующий уровень доходности от внедрения прогрессивных технологий и сформировать основу обеспечения экономической безопасности предприятия в условиях цифровизации. Однако его внедрение влечет за собой риски и угрозы, для нивелирования которых необходимо разрабатывать действенную систему управления.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Geng, Tongtong The business model of intelligent manufacturing with Internet of Things and machine learning // Enterprise information systems. 2022. No 2. Pp. 307-325.
2. Liu, Tze-Chang Digital policy in European countries from the perspective of the Digital Economy and Society Index // Policy and internet: an international journal of public policy. 2022. Vol. 14, No 1. Pp. 202-218.
3. Zdravković, Milan AI-enabled Enterprise Information Systems for Manufacturing // Enterprise information systems. 2022. Vol. 16, No 4. Pp 668-720.
4. Андреева М.А. О повышении эффективности управления на основе концепции промышленного интернета вещей // Автоматизация, телемеханизация и связь в нефтяной промышленности. 2020. № 12 (569). С. 33-37.
5. Enterprise digital transformation: technology, tools, and use cases / edited by Sathyan Munirathinam, Peter Augustine, Pethuru Raj. Boca Raton: Auerbach, 2022. 398 p.
6. Pandey, Omkant An Approach for Multi-Level Visibility Scoping of IoT Services in Enterprise Environments // IEEE transactions on mobile computing. 2022. Vol. 21, No 2. Pp. 408-420.
7. Elbadry, Mohammed Towards Fine-Grained Access Control in Enterprise-Scale Internet-of-Things // IEEE transactions on mobile computing. 2021. No 8. Pp. 2701-2714.