прозрачностью делают его более устойчивым к взлому, мошенничеству и коррупции. Благодаря успешным внедрениям, таким как TradeLens от IBM, становится ясно, что технология блокчейна может революционизировать то, как мы ведем бизнес и управляем данными.

**Список использованных источников**


1. Тапскотт, Д., и Тапскотт, А. (2016). Блокчейн-революция: как технология, лежащая в основе биткойнов, меняет деньги, бизнес и мир. Пингвин.
2. Лебедь, М. (2015). Блокчейн: проект новой экономики. О'Рейли Медиа, Инк.
3. Яо Л., Лю З., Хуанг Ю. и Чжан Ю. (2019). Система управления логистикой на основе блокчейна. В Международной конференции по смарт-блокчейну (стр. 174-182). Спрингер, Чам.
4. Иванов, Д. (2017). Технология блокчейн как потенциальный драйвер эффективности цепочки поставок. Транспортные исследования, часть E: Обзор логистики и транспорта, 98, 337–349.
5. Кшетри, Н. (2018). Роль блокчейна в достижении ключевых целей управления цепочками поставок. Международный журнал управления информацией, 39, 80-89.
6. Ван, С., Ван, Дж., Чжан, Д., Ли, Д., и Чжан, К. (2018). Промышленный интернет вещей на основе блокчейна: всесторонний обзор. Доступ IEEE, 6, 5836-5852.
7. Ляо, С. Х., Ченг, Ч. Х., и Чен, П. Ю. (2019). Блокчейн как сервис для управления цепочками поставок и его критические факторы успеха. Журнал промышленной информационной интеграции, 13, 37-44.



УДК 733.681


## УПРАВЛЕНИЕ КИБЕРФИЗИЧЕСКИМИ РИСКАМИ В ЦИФРОВЫХ ЦЕПОЧКАХ ПОСТАВОК


**Исаева Диана Рахатовна**
*diana.issayeva08@gmail.com*
Магистрант кафедры «Организация перевозок, движения и эксплутация транспорта»
ЕНУ им. Л.Н. Гумилева, Астана, Казахстан
Научный руководитель - А.А. Баубек



**Аннотация:** Цель данного исследования заключается в выявлении текущих проблем, связанных с вопросами безопасности и доверия в цифровых цепочках поставок. Развитие информационных и коммуникационных технологий (ИКТ) улучшило эффективность цепочек поставок, при этом создавая новые уязвимости и увеличивая вероятность возникновения угроз безопасности. Предыдущие исследования не уделяли должного внимания физическому аспекту безопасности, поэтому акцент сделан на безопасности кибер-физических систем. Для достижения цели исследования были изучены традиционные и цифровые цепочки поставок, их риски безопасности и основные различия. Разработана структура безопасности для киберфизических рисков в цифровых цепочках поставок.



**Ключевые слова:** киберфизические системы; цифровая цепочка поставок; безопасность информационно-коммуникационных технологий; малые и средние предприятия.

Развитие информационно-коммуникационных технологий (ИКТ) достигло стадии, когда оно является основой для других отраслей. Эта технологическая зависимость несет определенные риски, которые требуют решения с использованием соответствующих мер безопасности. С увеличением технологического прогресса сложно для ИТ-специалистов становится все труднее отслеживать тенденции, стандарты и передовую практику. Поэтому разрабатываются различные отраслевые структуры, которые могут служить руководством по соблюдению стандартов и общему пониманию передовой практики. Логистика - одна из отраслей, нуждающихся в разработке инфраструктуры. В связи с непрерывной цифровизацией грузовые контейнеры оснащаются различными интеллектуальными технологиями, что усиливает потребность в разработке системы киберфизической безопасности для цифровой цепочки поставок.

Цепочка поставок тесно связана с логистикой, транспортом и закупками, хотя эти термины часто смешиваются. Определение цепей поставок включает в себя планирование, координацию и контроль материалов от поставщика к потребителю. Этапы в цепи поставок бывают восходящими и нисходящими.

Цифровые цепи поставок описываются в литературе как оцифрованные цепи, применяющие новейшие технологии. Они также могут быть описаны как ориентированные на клиента платформы, собирающие данные в режиме реального времени и создающие более ценные и доступные услуги. Основные технологии в цифровых цепочках поставок включают блокчейн, смарт-контракты, робототехнику, дополненную реальность, искусственный интеллект, большие данные, Интернет вещей и промышленный интернет вещей [1].

Основное различие между цифровыми и традиционными цепочками поставок заключается в том, что традиционные представляют линейное и иерархическое взаимодействие без подключения в режиме реального времени, в то время как цифровые взаимодействуют на многомерном нелинейном уровне [1]. Традиционные цепочки предназначены для управления логистикой и производством, в то время как цифровые имеют множество подключенных потоков поставок. Отмечается, что традиционные цепочки часто не учитывают рентабельность и риски [2].

Интеграция цифровых цепочек поставок приносит выгоды, такие как снижение затрат, повышение производительности, уменьшение рабочей силы, снижение вероятности ошибок и увеличение прибыли [3].Схематическое представление цифровых цепочек поставок можно рассматривать как дополнительный уровень технологии по сравнению с традиционными цепочками поставок. Представление, предложенное автором , показано на рисунке 1.

Предложение автора, объединяющее исследования литературы по традиционным и цифровым цепочкам поставок, заключается в определении цифровых цепочек поставок как набора процессов, направленных на эффективную реализацию с добавленной стоимостью с целью получения новых форм дохода и подходов к использованию технологий участниками цепочки поставок.

Цифровизация традиционных цепочек поставок также влечет за собой новые риски и вызовы, включая риски безопасности, связанные с внедрением новых цифровых решений. Для минимизации этих рисков необходимы средства контроля безопасности, способные уменьшить уязвимости, угрозы и атаки на эти системы [4].

С развитием технологий и цифровизацией цепочек поставок возникает также нехватка соответствующих навыков у сотрудников [5]. Приблизительно 60% инцидентов безопасности происходят из-за некомпетентности сотрудников, чаще всего не намеренно, поэтому обучение сотрудников может решить эту проблему.

В цифровых цепочках поставок особое значение имеют блокчейн-решения, применимые в различных отраслях, например, в автомобилестроении, где блокчейн может поддерживать полный жизненный цикл автомобиля, включая отчеты о пробеге, страхование и техническое обслуживание. Блокчейн может быть эффективным инструментом, но необходимо учитывать

риски безопасности, такие как потеря закрытого ключа, внедрение вредоносных программ и надежность криптографического алгоритма [1]. С появлением новых, более стабильных и безопасных блокчейн-платформ эти риски могут быть снижены или даже устранены.

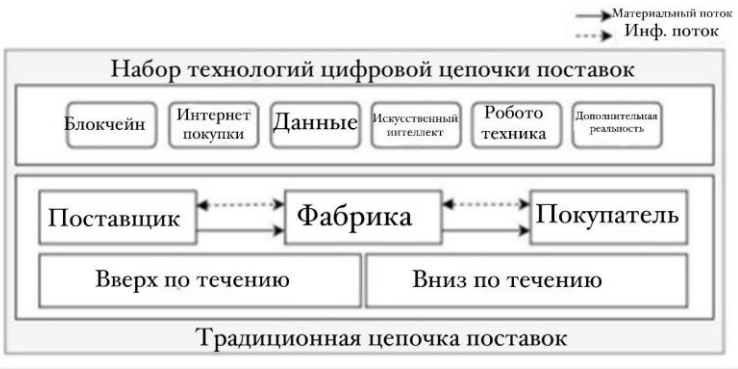


Рис. 1. Схематическое изображение цифровой цепочки поставок

Одним из наиболее признанных методов повышения безопасности в организации является управление рисками [1][2]. Это требует относительно большого объема ресурсов, но это принимается во внимание в контексте безопасности. Цель этого концепция безопасности призвана предоставить малым и средним предприятиям в цифровой цепочке поставок рекомендации по снижению киберфизических рисков.

Концепция безопасности основана на базовых процессах управления рисками:

1. идентификация;
2. оценка;
3. смягчение последствий и лечение;
4. мониторинг.

Идентификация рисков безопасности является первым шагом в управлении рисками. Идентификация рисков - это учет всех потенциальных рисков в организации. Категоризация рисков является одним из наиболее важных шагов в процессе идентификации рисков.

Согласно проведенному исследованию, классификация рисков системной безопасности предоставляет компаниям возможность осознать, какие риски оказывают наибольшее воздействие на их активы и какие уязвимости являются наиболее подверженными. Эта классификация позволяет заинтересованным сторонам создать бизнес с минимальным количеством уязвимостей, насколько это возможно. Предложенный авторами классификатор рисков представляет собой гибридный инструмент, который, в отличие от других, обеспечивает более точную и всестороннюю классификацию рисков, учитывая разнообразие систем. Этот классификатор основан на следующих факторах: источнике риска, агенте, мотивации, намерении и воздействии.

Авторы предлагают разделение рисков безопасности информационных систем на три подкласса: антропогенные, обусловленные окружающей средой и обусловленные технологиями. Основными классами являются внутренние и внешние риски. Класс техногенных рисков включает угрозы, создаваемые деятельностью человека, такие как хакеры, которые могут представлять опасность для систем через кибератаки. Экологические риски - это риски, не зависящие от вмешательства человека, такие как стихийные бедствия, войны и терроризм. Риски, связанные с технологией, возникают в результате физических или химических процессов.

С учетом того, что обеспечение безопасности информационных систем является важной задачей, предложенная классификация рисков облегчает понимание их происхождения и, следовательно, разработку стратегии по снижению рисков безопасности.В. Оценка рисков

Вторым этапом в процессе управления рисками является оценка рисков, и правильная оценка рисков безопасности играет ключевую роль в реализации стратегий по снижению рисков. Стандарты серии IEC 62443, придерживающиеся основной концепции промышленной кибербезопасности как составной части безопасности киберфизических систем [2], подчеркивают, что оценка рисков должна включать три основные составляющие:

1. Функциональная безопасность: В этой части оценка включает в себя мониторинг устройств и защиту от случайных сбоев, которые могут привести к неожиданным сбоям в работе устройства.

2. Физическая безопасность: Включает риски, связанные с окружающей средой, а также стихийные бедствия, которые могут оказать воздействие на физические аспекты системы.

3. Кибербезопасность: Этот аспект касается безопасности кибернетической среды или сети, включая устройства, программное обеспечение, процессы и информацию. В контексте киберфизических систем он направлен на решение проблем безопасности при сборе, обработке и совместном использовании информации в обширной автономной сетевой среде.

Как и в случае с управлением рисками, основные принципы кибербезопасности могут быть определены как защита, сдерживание и развитие. Важно понимать, что кибербезопасность не может быть самостоятельной целью, а представляет собой неотъемлемую часть общей безопасности цепочки поставок.

В исследовании рассмотрены методы оценки рисков безопасности для киберфизических систем, выявлены четыре подходящих метода из 13, получивших наивысшую оценку. Для малых и средних предприятий предпочтительным является метод STPA-SafeSec, обеспечивающий всесторонний анализ рисков с ограниченными ресурсами и динамический анализ в реальном времени.

Для крупных компаний или тех, у кого есть достаточные ресурсы, рекомендуется байесовская сетевая модель , использующая теорему Байеса для вычисления вероятности в соответствии с условной зависимостью. Важно отметить, что гибридная Байесовская сетевая модель не рассматривалась и могла бы быть альтернативой без исторических данных.

В критически важных цепочках поставок, например, в ядерной энергетике, предпочтительны стандарты IEC 61508 , а в цифровых цепочках с акцентом на цифровые риски - система кибербезопасности от Национального института стандартов и технологий [7].

Оценка рисков киберфизических систем в основном фокусируется на системной перспективе, предостерегая о недостаточном внимании к стороне пользователя. Рекомендуется уделить дополнительное внимание участию пользователей, особенно при хранении физически конфиденциальной информации, где обеспечение конфиденциальности, целостности и доступности часто требует использования физических средств защиты.

Вовлечение в оценку рисков внешних специалистов, специализирующихся на управлении рисками, становится все более практичным, хотя такой подход может быть более затратным.

Снижение рисков является важным компонентом устойчивого управления рисками. Оно охватывает процессы и руководящие принципы, которые компании внедряют для минимизации потенциальных инцидентов безопасности или уменьшения ущерба, который они могут причинить.

Устранение рисков является наиболее эффективным, но часто и самым дорогостоящим способом снижения рисков [6]. Эффективно разработанная стратегия управления рисками с акцентом на методы снижения рисков может предотвратить риски до 55% в инфраструктуре киберфизических систем [5].

Согласно исследованиям типы киберфизических атаки можно разделить на следующие категории:

1. сбои в обслуживании;
2. кибершпионаж;
3. деструктивные действия и саботаж;
4. крупномасштабные киберконфликты.

В таблице I перечислены возможные методы снижения рисков безопасности для этих категорий атак.

Таблица I

СТРАТЕГИИ СМЯГЧЕНИЯ ПОСЛЕДСТВИЙ АТАК

| **Категория атаки** | **Методы снижения рисков** |
|---|---|
| Сбои в обслуживании | Сетевая инфраструктура (например, брандмауэр и балансировка нагрузки); выявление аномалий или отклонений [30]; защита сети [31]; DDoS как услуга и программное обеспечение для защиты от вредоносных программ. |
| Кибершпионаж | Механизмы контроля доступа (например, двухфакторная аутентификация); шифрование файлов [30]. |
| Деструктивные действия и саботаж | Физическая безопасность и видеонаблюдение; системы обнаружения и предотвращения вторжений ; расширенный мониторинг сотрудников, подверженных высокому риску; разработка политики предотвращения потери данных [32]; многоуровневая модель безопасности active directory. |
| Крупномасштабные киберконфликты | кибердипломатия [33]. |

Для каждой категории атак эти методы снижения рисков дополняют друг друга, обеспечивая, таким образом, наилучшие методы совместного управления рисками и минимизируя потенциальные киберфизические риски. Разработанная система безопасности цифровой цепочки поставок схематично показана на рисунке 2.

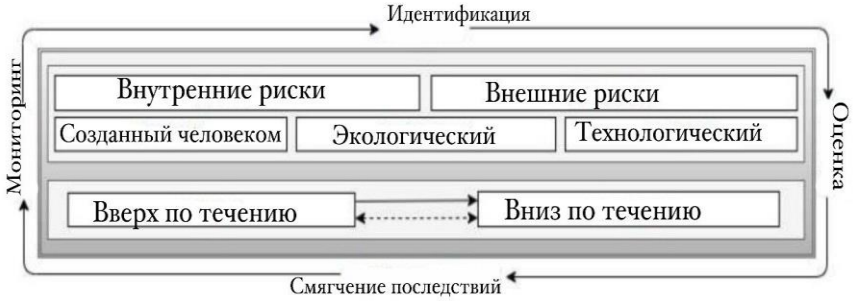


Рис. 2. Система безопасности цифровой цепочки поставок

Мониторинг и оценка уровней риска также рекомендуются для обновления старых стратегий, которые, возможно, оказались недостаточно эффективными. Рекомендуется постоянно выполнять все шаги по управлению рисками, поскольку допуски к риску, затраты на профилактику и уровни серьезности могут меняться, чтобы обеспечить максимально возможный уровень безопасности [8].

Киберфизические системы должны быть самоустойчивыми к кибератакам, и этого можно достичь с помощью хорошо продуманной стратегии оценки рисков и их смягчения.

По мере продолжения исследований в будущем следует учитывать экономическое воздействие киберфизических систем и устройств Интернета вещей и их безопасность . Такие междисциплинарные исследования были бы полезны в будущем, как при

проектировании "умных городов", так и при разработке решений для умной мобильности, которые являются активным объектом исследований. Исследование повысит ценность за счет интеграции оценки экономического воздействия и кибербезопасности модели, которые ранее не рассматривались вместе.

**Список использованных источников**

[1] SwissRE Institute, “De-risking global supply chains: rebalancing to strengthen resilience,” no. 6, 2020.

[2] van H. Remko, “Research opportunities for a more resilient postCOVID-19 supply chain – closing the gap between research findings and industry practice,” Int. J. Oper. Prod. Manag., vol. 40, no. 4, pp. 341–355, 2020, doi: 10.1108/IJOPM-03-2020-0165.

[3] S. K. Paul, P. Chowdhury, M. A. Moktadir, and K. H. Lau, “Supply chain recovery challenges in the wake of COVID-19 pandemic,” J. Bus. Res., vol. 136, no. August, pp. 316–329, 2021, doi: 10.1016/j.jbusres.2021.07.056.

[4] B. Tabrizi, “Digital Transformation Is Not About Technology,” 2019. https://hbr.org/2019/03/digital-transformation-is-not-abouttechnology.

[5] Michigan State University, “Is Logistics the Same as Supply Chain Management?,” 2020. https://www.michiganstateuniversityonline.com/resources/supplychain/is-logistics-the-same-as-supply-chain-management/ (accessed Feb. 04, 2021).

[6] Graham C. Stevens, “International Journal of Physical Distribution & Logistics Management Emerald Article: Integrating the Supply Chain,” Int. J. Phys. Distrib. Logist. Manag., vol. 19, no. 8, pp. 3–8, 1989.

[7] B. Ageron, O. Bentahar, and A. Gunasekaran, “Digital supply chain: challenges and future directions,” Supply Chain Forum, vol. 21, no. 3, pp. 133–138, 2020, doi: 10.1080/ 16258312 .2020.1816361.

[8] The Center of Global Enterprise, “Digital Supply Chains: A Frontside Flip.” 2015.

ӘОЖ 568

## КӘСІПОРЫННЫҢ ЖҰМЫСЫН ЖАҚСАРТУ ҮШІН ЛОГИСТИКАҒА ЖАСАНДЫ ИНТЕЛЛЕКТТІ ЕНГІЗУ

**Қайрбек Лаула Ержанқызы**
*Laulaqueen8@gmail.com*
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, «Көлік-энергетикалық» факультетінің магистранты
Ғылыми жетекші – С.Н. Нураков

**Аннотация.** Бұл мақалада Қазақстанның логистикалық саласында ЖИ қолдану жағдайға қалай әсер ететіні және осы салада ЖИ қолданудың оң және теріс жақтары қарастырылады. Ол сондай-ақ Қазақстан логистикасында ЖИ пайдалануды жақсарту туралы идеяларды ұсынады. Негізгі мақсат - ЖИ қолдану Қазақстанның логистикасына қалай әсер ететінін көру. Нақты мақсаттар -Қазақстан логистикасында ЖИ қай жерде пайдалы болуы мүмкін екенін, Қазақстан логистикасында ЖИ қандай проблемалар тудыратынын, Қазақстан логистикасында ЖИ қалай жақсартуға болатынын анықтау. Зерттеуде сандар да, әңгімелер де қолданылды: көптеген адамдарға сұрақтар қою үшін сауалнамалар және адамдардың пікірін тыңдау үшін сұхбаттар. Зерттеу ЖИ процесті жылдамдату, ақша табудың көбірек жолдарын жасау және Қазақстан экономикасына көмектесу арқылы логистиканы жақсарта алатынын