DOI 10.37882/2223-2966.2024.03.30

АВТОМАТИЗИРОВАННАЯ КИБЕРУСТОЙЧИВАЯ СИСТЕМА НА ПИЩЕВЫХ ПРЕДПРИЯТИЯХ

AUTOMATED CYBER-RESISTANT SYSTEM IN FOOD ENTERPRISES

S. Sidorin

Summary. In the modern global space, a digital revolution is currently taking place, the results of which contribute to the implementation and adaptation of digital technologies, machine learning methods and cyber-resistant systems in a manufacturing enterprise. Since the food industry is currently developing under the influence of the constant use of digital technologies, it is advisable to touch upon the topic of developing an automated cyber-resistant system in food enterprises. The aim of the article was to present a review of the literature on cybersecurity in food enterprises, based on a vertical approach, in order to identify the main topics and areas that characterize cybersecurity in the food service industry in the Industry 4.0 paradigm, and to propose a proprietary cyber-resilient system for food enterprises, which was achieved during the research process. The author's concept of an automated cyber-sustainable system in food enterprises was presented, which includes four elements: ICT, artificial intelligence method, supply chain automation and robotization of the production process. Each of the above components works under the influence of the principles of a cyber-sustainable system, which were highlighted in the context of the research: the principle of integration of production processes; use of additional sensors and the Internet of things; machine learning, big data analysis; robotization of production at food enterprises; production planning and management.

Keywords: automated cyber-resistant system, food enterprises, digital revolution, principles, technologies, threat to cybersecurity, cyber attacks and vulnerability.

Сидорин Сергей Юрьевич
Московский авиационный институт (национальный исследовательский университет)
sarmatsid@yandex.ru

Аннотация. В современном глобальном пространстве на данный момент происходит цифровая революция, результаты которой способствуют внедрению и адаптации на производственном предприятии цифровых технологий, методов машинного обучения и киберустойчивых систем. Так как пищевая промышленность развивается в настоящее время под воздействием постоянного использования цифровых технологий, целесообразно затронуть тему разработки автоматизированной киберустойчивой системы на пищевых предприятиях. В статье была поставлена цель — представить обзор литературы по кибербезопасности на пищевых предприятиях, основанный на вертикальном подходе, для того чтобы выявить основные темы и области, характеризующие кибербезопасность в отрасли общественного питания в парадигме Индустрии 4.0, и предложить авторскую киберустойчивую систему для пищевых предприятий, которая была достигнута в процессе исследования. Была приведена авторская концепция автоматизированной киберустойчивой системы на пищевых предприятиях, включающая четыре элемента: ИКТ, метод искусственного интеллекта, автоматизация цепочек поставок и роботизация производственного процесса. Каждая из приведенных составляющих работает под воздействием принципов киберустойчивой системы, которые были выделены в контексте проводимого исследования: принцип интеграции производственных процессов; использование дополнительных датчиков и Интернета вещей; машинное обучение, анализ больших данных; роботизация производства на пищевых предприятия; планирование и управление производством.

Ключевые слова: автоматизированная киберустойчивая система, пищевые предприятия, цифровая революция, принципы, технологии, угроза кибербезопасности, кибератаки и уязвимость.

Введение

Пищевая промышленность представляет собой сложную и многомерную отрасль и в то же время перспективный сектор, который ориентирован на производство сырья, полуфабрикатов и готовой продукции. В него входят компании, которые производят, перерабатывают, продают и доставляют продукты питания, напитки и пищевые добавки [1].

Происходящая в мире цифровая революция влияет на пищевую промышленность и характеризуется моделью массового производства продуктов питания. Складывающаяся индустрия 4.0 предполагает внедрение промышленными компаниями технологий и процессов, усовершенствованных благодаря цифровизации, для получения конкурентных преимуществ на внутреннем и глобальном рынках [2].

Предприятия ресторанно-гостиничного бизнеса могут извлечь выгоду из практического использования технологических ресурсов для удовлетворения потребностей населения мира в продовольственных продуктах в соответствии с принятыми нормами здравоохранения, безопасности пищевых продуктов и законодательства. Эти технологии применяются на нескольких этапах производства продуктов питания и напитков, таких как выращивание, транспортировка, обработка, а также упаковка и хранение пищевых продуктов. В частности, в последние годы концепция киберустойчивой системы позволила усовершенствовать деятельность предприятий в сфере общественного питания. Киберустойчивые системы полагаются на промышленный Интернет вещей, что обусловлено работой взаимосвязанных датчиков, приборов и дополнительных технических устройств, объединенных в сеть, включая производство и управление энергопотреблением [3].

Киберустойчивая система применяется в индустрии общественного питания благодаря использованию подключенных датчиков и контроллеров на предприятиях, инновационных способов для оптимизации обработки и принятия оперативных решений. При этом Интернет вещей вызвал существенные опасения в отношении кибербезопасности, включая риски, последствия которых выходят за рамки взаимодействия информационных систем с физическим миром [3].

Таким образом, необходимо принять адекватные меры защиты для предотвращения кибератак, которые могут изменить правильную работу предприятий с последующим потенциальным экономическим и социальным риском [1]. Кибербезопасность предполагает не только защиту информационных ресурсов от любых кибератак, но и других активов, таких как человеческие ресурсы, и, следовательно, выходит за рамки традиционной концепции информационной безопасности от киберугроз в киберпространстве [4].

Риск для сектора общественного питания становится все более значительным, о чем свидетельствуют многочисленные произошедшие киберпреступления. Так, в июне 2017 года программа-вымогатель (одна из наиболее распространенных причин киберугроз), известная как «Petya», заразила более 2000 компаний по всему миру, и впервые это коснулось индустрии общественного питания. Жертвами нападения стали компания Mondelez в США и фабрика Cadbury в Тасмании [5].

Интерес к теме возникает также из различных дискуссий исследователей, рассматривающих проблему с практической точки зрения. С.Ю. Сидорин и соавт., обсуждая, что такое кибербезопасность, признали продовольствие и сельское хозяйство одним из важнейших секторов сетевой, киберустойчивой инфраструктуры [6]. Г.А. Попов и К.Н. Штонда, обсуждая программы-вымогатели и безопасность цифровой пищевой цепи, пришли к выводу, что продовольственной и сельскохозяйственной системе нужно устранить пробелы в образовании, инвестициях и информационной прозрачности в области кибербезопасности [7].

А. Алькьюхаиби в соавт. обсуждали угрозы кибербезопасности для цепочки поставок продовольствия, выделяя, по крайней мере, три канала атак: хактивистские, ответственные за DDoS-атаки для защиты окружающей среды и животных от воздействия на производство продуктов питания, локально групповые, где несколько киберпреступников участвует в атаках с целью кражи информации, глобально групповые, где значительные по масштабу группировки (национального масштаба), участвуя в политических действиях, осуществляют кибератаки с целью снижения международного суверенитета конкретной страны [8]. А. Телукдарие в соавт. обсуждали низкую зрелость кибербезопасности в африканском секторе общественного питания, сообщая точку зрения вице-президента фирмы, занимающейся кибербезопасностью, которая заявила о необходимости усовершенствовать технологические элементы, способные защитить взаимосвязанную систему производства продуктов питания [9].

И.В. Машкина и И.Р. Гарипов обсудили потенциальные последствия кибератаки на систему промышленного контроля пищевых продуктов: загрязнение пищевых продуктов, угрожающее здоровью населения, физический вред работникам, увеличение износа оборудования, ущерб окружающей среде и существенные финансовые потери для компаний [10].

А. Алькьюхаиби в соавт. предоставили руководство по измерению риска кибербезопасности, обусловливающего последствия и угрозы во взаимодействии нескольких сторон в организационно-хозяйственной деятельности: чтобы риск существовал, все три фактора (уязвимость, последствия, угрозы) должны быть больше нуля [11]. А. Алькьюхаиби в соавт. обсудили анализ, предоставленный GlobalData, согласно которому доля производителей продуктов питания, нанимающих сотрудников в области кибербезопасности возросла с 29,7 % в феврале 2021 года до 44,6 % в феврале 2022 года, и пришли к выводу, что компании, инвестирующие в кибербезопасность, будут лучше подготовлены к преодолению в дальнейшем непредвиденных (сложно прогнозируемых) обстоятельств [12].

Актуальность работы

На сегодняшний день существует достаточно мало научных исследований, где авторы анализировали достижения в области кибербезопасности в индустрии общественного питания и предлагали собственные концепции киберустойчивых систем. Тем не менее, среди публикаций по специфике кибербезопасности в академической литературе особую значимость имеет исследование [13], поскольку оно описывает современные способы решения проблем кибербезопасности в парадигме Индустрии 4.0, которая широко использовалась в индустрии общественного питания. Однако структурные характеристики пищевых предприятий, применяемые ими цепочки поставок и задействованные продукты создают особый контекст и ситуации, которые подразумевают практическую реализацию стратегических направлений и решений в области кибербезопасности, что приводит к пробелам в существующих исследованиях. Учитывая важность кибербезопасности в отрасли общественного питания и современного общества в целом, в данном исследовании представлен обзор литературы по кибербезопасности на пищевых предприятиях, основанный на вертикальном подходе, для того чтобы

выявить основные темы и области, характеризующие кибербезопасность в отрасли общественного питания в парадигме Индустрии 4.0, и предложить авторскую киберустойчивую систему для пищевых предприятий. Этот обзор исследований отражает современное состояние кибербезопасности, предлагая отраслевой уровень знаний, который может описать, как существующие подходы решают проблемы кибербезопасности в отрасли общественного питания.

Следовательно, цель данного исследования — представить обзор литературы по кибербезопасности на пищевых предприятиях, основанный на вертикальном подходе, для того чтобы выявить основные темы и области, характеризующие кибербезопасность в отрасли общественного питания в парадигме Индустрии 4.0, и предложить авторскую киберустойчивую систему для пищевых предприятий.

Задачи исследования:

1. Представить обзор литературы по кибербезопасности на пищевых предприятиях, основанный на вертикальном подходе.
2. Выявить основные темы и области, характеризующие кибербезопасность в отрасли общественного питания в парадигме Индустрии 4.0.
3. Предложить авторскую киберустойчивую систему для пищевых предприятий.

Материалы и методы

Для представления обзора литературы по кибербезопасности на пищевых предприятиях, основанного на вертикальном подходе, автором статьи был проведён анализ научно-прикладной литературы.

Помимо метода обзора и анализа научно-прикладной литературы, автором статьи использовался метод индукции, дедукции, систематизации, графического представления информации, абстрактно-логический метод, метод построения автоматизированной киберустойчивой системы.

Результаты и их обсуждение

В процессе проведения исследования был сделан обзор литературы по кибербезопасности на пищевых предприятиях, результаты которого отражены в блоках введения и актуальности работы данной статьи. Систематический обзор литературы позволил выделить основные темы и области, характеризующие кибербезопасность в отрасли общественного питания:

1. Автоматизированная киберустойчивая система;
2. Уязвимость и кибератаки;
3. Цифровая революция отрасли общественного питания;
4. Использование парадигмы Индустрии 4.0 в развитии отрасли общественного питания;
5. Специфика работы пищевых предприятий.

В связи с имеющейся актуальностью и практической значимостью поднимаемого в статье вопроса автор разработал концепцию автоматизированной киберустойчивой системы для пищевых предприятий, которая приведена на рисунке 1.

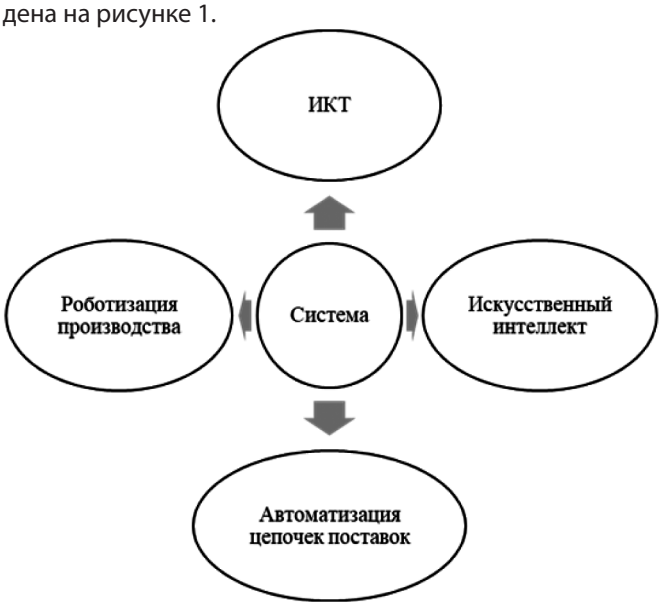

Рис. 1. Концепция автоматизированной киберустойчивой системы для пищевых предприятий
Источник: разработано автором.

Составляющими автоматизированной киберустойчивой системы пищевых предприятий выступают:

1. Методы искусственного интеллекта, позволяющие осуществлять спектр работ машинного обучения и анализировать значительные массивы данных;
2. Роботизация пищевого производства необходима для ускорения происходящих в пищевом производстве бизнес-процессов, оптимизации действий при реализации производства;
3. ИКТ способствуют интеграции производственных процессов, использованию дополнительных датчиков и Интернета вещей;
4. Автоматизация цепочек поставок подразумевает оптимальное планирование и управление производством.

Помимо проиллюстрированной на рисунке 1 концепции автоматизированной киберустойчивой системы для пищевых предприятий, предлагаются принципы её работы, представленные в таблице 1.

Исходя из представленных в таблице 1 принципов, преимущества автоматизированной киберустойчивой системы для пищевых предприятий включают повыше-

Таблица 1.

Принципы работы концепции автоматизированной киберустойчивой системы для пищевых предприятий

Принцип	Содержание
Принцип интеграции производственных процессов	Объединение автоматизированной киберустойчивой системой всех этапов производства, включая поставки продукции, доставку готового результата. Принцип позволяет регулировать деятельность любых производственных подразделений, а также оптимизировать производственные бизнес-процессы
Использование дополнительных датчиков и Интернета вещей	Сбор данных о современном состоянии производственного оборудования, качестве материалов, влажности, температуре в помещениях, что способствует своевременному реагированию на изменения в реальном времени, предупреждать возможные проблемы
Машинное обучение, анализ больших данных	Посредством встроенных в киберустойчивую систему алгоритмов можно оптимизировать производственные процессы, смоделировать потребительский спрос, оптимально управлять запасами, а также реализовывать оптимальную производственную стратегию и направления по снабжению
Роботизация производства на пищевых предприятиях	Исполнение рутинных задач, например, сортировка и упаковка продукции, а также подача готовой продукции
Планирование и управление производством	Оптимизация производственного планирования, рациональное управление запасами, транспортной логистики и производственного контроля

Источник: разработано автором.

ние эффективности производства, снижение затрат, увеличение качества и безопасности продукции, сокращение времени реакции на изменения рыночных условий, а также повышение конкурентоспособности пищевого предприятия в целом.

Выводы

В исследовании был представлен обзор литературы по кибербезопасности на пищевых предприятиях, основанный на вертикальном подходе.

Выявлены основные темы и области, характеризующие кибербезопасность в отрасли общественного питания в парадигме Индустрии 4.0.

Предложена авторская автоматизированная киберустойчивая система для пищевых предприятий.

ЛИТЕРАТУРА

1. Luque A. et al. State of the Industry 4.0 in the Andalusian food sector // Procedia Manufacturing. — 2017. — Vol. 13. — P. 1199-1205.
2. Castelo-Branco I., Cruz-Jesus F., Oliveira T. Assessing Industry 4.0 readiness in manufacturing: Evidence for the European Union // Computers in Industry. — 2019. — Vol. 107. — P. 22–32.
3. Boye A.C., Kearney P., Josephs M. Cyber-risks in the industrial internet of things (IIoT): Towards a method for continuous assessment // Information Security: 21st International Conference, ISC 2018, Guildford, UK, September 9–12, 2018, Proceedings 21. — Springer International Publishing, 2018. — P. 502–519.
4. Von Solms R., Van Niekerk J. From information security to cyber security // Computers & security. — 2013. — Vol. 38. — P. 97–102.
5. Latino M.E., Menegoli M. Cybersecurity in the food and beverage industry: A reference framework // Computers in Industry. — 2022. — Vol. 141. — P. 103702.
6. Сидорин С.Ю., Благовещенский И.Г., Соболева Е.А., Шармаев В.И. Киберустойчивость предприятий пищевой промышленности: определение потенциальных векторов атаки // Вопросы защиты информации. — 2023. — № 3. — С. 51–58.
7. Попов Г.А., Штонда К.Н. Процедура оценки информационной безопасности АСУТП на основе классификации важности показателей // Вестник АГТУ. — 2008. — № 1 (42). — С. 66–73.
8. Alqudhaibi A. et al. Cybersecurity 4.0: safeguarding trust and production in the digital food industry era // Discover Food. — 2024. — Vol. 4. — No. 1. — P. 1–18.
9. Telukdarie A. et al. Industry 4.0 Technological Advancement in the Food and Beverage Manufacturing Industry in South Africa—Bibliometric Analysis via Natural Language Processing // Information. — 2023. — Vol. 14. — No. 8. — P. 454.
10. Машкина И.В., Гарипов И.Р. Разработка EPC-моделей угроз нарушения информационной безопасности автоматизированной системы управления технологическими процессами // Безопасность информационных технологий. — 2019. — Т. 26. — №. 4. — С. 6–20.
11. Alqudhaibi A. et al. Safeguarding food industry: understanding cyberthreats and ensuring cybersecurity // Engineering Proceedings. — 2023. — Vol. 40. — No. 1. — P. 11.
12. Alqudhaibi A. et al. Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations // Sensors. — 2023. — Vol. 23. — No. 9. — P. 4539.
13. Latino M.E., Menegoli M. Cybersecurity in the food and beverage industry: A reference framework // Computers in Industry. — 2022. — Vol. 141. — P. 103702.

Журнал «Современная наука: актуальные проблемы теории и практики»