Шаргородский К.В., Смелянец Н.А., Вершигора Е.В.
магистры,
Одесская национальная академия связи имени А.С. Попова

КИБЕРУСТОЙЧИВОСТЬ ЦИФРОВЫХ ПРЕДПРИЯТИЙ КОНЦЕПЦИИ ИНДУСТРИЯ 4.0

Концепция Индустрия 4.0, или «четвертая промышленная революция», впервые сформулирована в 2011 году и по своей сути описывалась как средство повышения конкурентоспособности предприятий Германии путем интеграции киберфизических систем в заводские процессы. Как отмечается в [1], индустрия 4.0 – это новый виток промышленной революции, который характеризуется интеграцией производства и сетевых коммуникаций. Новое поколение оборудования позволяет собирать данные в реальном времени, производить персонализированные продукты, создавая прямые связи цепочки производства от заказа продукта до получения его потребителем в кратчайшие сроки с максимальной эффективностью процесса. Стоит отметить, что в идеологии Индустрия 4.0 закладывается модель, при которой системы объединяются в одну сеть, связываются друг с другом, самостоятельно настраиваются и учатся новым моделям поведения.

К технологиям «четвертой промышленной революции» часто относят большие данные (big data), интернет вещей (IoT), виртуальную и дополненную реальность, 3D-печать, квантовые вычисления и блокчейн. Технологии дают новые возможности, но при этом способствуют появлению новых угроз и рисков, в том числе, в направлении АСУ-ТП и объектов критической инфраструктуры [2].

По мере возрастания сложности современных киберсистем, у них возникают новые все более эмерджентные (от англ. emergent – возникающий, неожиданно появляющийся) системные свойства: киберустойчивость, управляемость, самоорганизация, проактивная кибербезопасность и адаптивность. Киберустойчивость (англ. Cyber Resilience) является важнейшим свойством любой киберсистемы, особенно в условиях перехода к Индустрии 4.0. В отличие от кибербезопасности с ориентацией на оценку вероятности возникновения инцидентов и предотвращение возможных угроз безопасности, обеспечение киберберустойчивости в большей степени направлено на

сохранение целевого поведения и работоспособности киберсистем в условиях множества кибератак [3].

Рис. 1. Эволюция моделей киберустойчивости

Современные киберсистемы не обладают требуемой киберустойчивостью (Cyber Resilience) для функционирования в условиях разнородных, массовых кибератак из-за высокой структурной и функциональной сложности названных систем, потенциальной опасности имеющихся уязвимостей и «цифровых бомб». Кроме того, все еще недостаточно эффективны современные средства кибер-безопасности, в том числе средства антивирусной защиты, сканеры уязвимостей, а также системы обнаружения, предупреждения и нейтрализации компьютерных атак. Применяемые классические методы и средства обеспечения надежности (Reliability) и отказоустойчивости (Response and Recovery), использующие возможности структурной и функциональной избыточности, N-кратного резервирования, эталонирования и реконфигурации уже не пригодны для обеспечения требуемого уровня киберустойчивости (Cyber Resilience) и предотвращения катастрофических последствий требуется новая парадигма построения корпоративной системы обеспечения киберустойчивости, которая будет способна своевременно предупреждать и упреждать кибератаки, а в случае кибернападения – «смягчить» удар, снизить его силу деструктивного воздействия и минимизировать последствия. Такая система защиты должна базироваться на понятии управлении непрерывности бизнеса (BCM – Business Continuity Management) и позволять жертвовать некоторыми функциями и компонентами инфраструктуры для возобновления бизнеса [4]. На рис. 2 показана система управления киберустойчивостью в аспекте угроз и рисков цифровых предприятий.

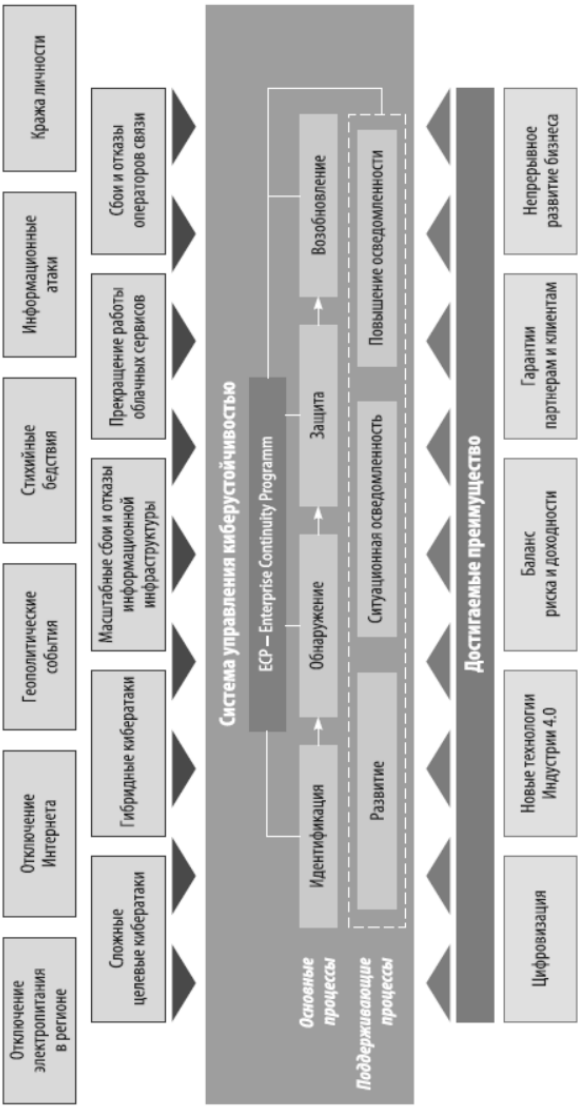

Рис. 2. Система управления киберустойчивостью в аспекте угроз и рисков цифровых предприятий

Стоит отметить, что сегодня спектр угроз прерывания бизнеса достаточно широк и постоянно увеличивается. Например, прерывания бизнеса могут быть вызваны постановлениями судов из-за допущенных нарушений в части защиты окружающей среды или трудового законодательства, негативными действиями или бездействиями контрагентов и партнеров по бизнесу, забастовками и акциями протеста сотрудников, инцидентами кибербезопасности и пр. По этим причинам компаниям исключительно важно не ограничиваться требованиями международных стандартов ISO 9001, ISO 14001, ISO 45001, ISO/IEC 27001 и др. для предупреждения возможных негативных инцидентов, но и обеспечить такие условия, при которых возможно гарантированно продолжить свою деятельность (возможно, с потерей ряда функций) в случае наступления чрезвычайных событий.

Список использованных источников:

1. Макаревич А. Индустрия 4.0: Какие перемены грядут на рынке услуг [Електронний ресурс] / Алина Макаревич // Delo.ua. – 2017. – Режим доступу: https://delo.ua/business/industrija-40-kakie-peremeny-grjadut-na-rynke-uslug-328161/

2. Кільдішев В.Й. Щодо захисту об’єктів критичної інфраструктури в аспекті сучасних загроз та ризиків / В.Й. Кільдішев, М.М. Гаджиєв, В.І. Вітрук, Е.Е. Мустафаєв // Матеріали 73-ї науково-технічної конференції професорсько-викладацького складу, науковців та студентів ОНАЗ ім. О.С. Попова. – 2018.

3. Петренко С.А. Управление киберустойчивостью / Сергей Анатольевич Петренко. – Санкт-Петербург: Издательский дом «Афина», 2019. – 200 с. (информационно-методическое пособие).

4. Семь шагов к непрерывности бизнеса [Електронний ресурс] // Habr. – 2015. – Режим доступу: https://habr.com/ru/company/softline/blog/261053