УДК 004.056

М.А. БАЕШОВ, А.Г. ЯРОВАЯ

*Национальный исследовательский ядерный университет «МИФИ», Москва*

# КИБЕРБЕЗОПАСНОСТЬ ПРИ ЦИФРОВОЙ ТРАНСФОРМАЦИИ МАЛОГО И СРЕДНЕГО БИЗНЕСА

В современных условиях цифровая трансформация малого и среднего бизнеса сопровождается внедрением облачных сервисов, дистанционных каналов продаж и автоматизации управленческих процессов, что резко увеличивает значимость цифровых активов и одновременно расширяет поверхность потенциальных киберугроз. Задача заключается в разработке адаптируемой и экономически оправданной стратегии кибербезопасности для МСБ, которая обеспечивает конфиденциальность, целостность и доступность данных, устойчивость бизнес-процессов к инцидентам (включая атаки типа ransomware), соблюдение нормативных требований и минимизацию затрат через приоритизацию мер и использование управляемых/облачных сервисов. Российская подготовка специалистов в области кибербезопасности фокусируется на интеграции теории и практики, что создаёт предпосылки для прикладных решений в рамках задач МСБ. [1]

Решение проблемы предлагается реализовать на трёх взаимосвязанных уровнях: организационном, процедурном и техническом. На организационном уровне необходимо назначение ответственного за информационную безопасность (включая возможность аутсорсинга функции к MSSP), внедрение регламентов управления доступом и требований к поставщикам, а также формализация плана реагирования на инциденты. На процедурном уровне ключевыми элементами являются инвентаризация и классификация цифровых активов, регулярный патч-менеджмент, проверяемые резервные копии с определёнными RTO/RPO и регулярные упражнения по восстановлению. Технические меры включают внедрение многофакторной аутентификации, управление привилегиями по принципу минимальных прав, сегментацию сети, базовый мониторинг и защиту конечных точек (EDR) с возможностью подключения облачного SIEM или MSSP при росте нагрузки. Комплексный подход должен опираться на стандарты и лучшие практики, адаптированные под ресурсные ограничения МСБ. [1]

Предлагается концепция «модульной минимальной защиты» как лёгкого для внедрения набора взаимодополняющих модулей безопасности: модуль идентификации и классификации активов, модуль

аутентификации и управления доступом, модуль резервирования и восстановления, модуль обучения персонала с симуляциями фишинга и модуль мониторинга с опцией быстрого подключения MSSP. Такой модульный подход позволяет масштабировать защиту по мере роста компании и гармонизировать её с образовательными практиками и лабораторными наработками профильных программ подготовки. [2]

Кибербезопасность при цифровой трансформации МСБ должна рассматриваться как интегральная часть бизнес-стратегии, а не как внешняя ИТ-опция. Для достижения баланса между эффективностью защиты и ограниченными ресурсами МСБ необходимо применять модульный, поэтапный подход: быстрые и высокоэффективные меры дают заметный прирост устойчивости бизнеса, а постепенное подключение мониторинга и профессиональных сервисов позволяет наращивать зрелость безопасности. Образовательная среда и практические наработки ведущих профильных программ создают методическую базу для воспроизводимых решений и пилотных проектов, которые могут быть масштабированы в отраслевом контексте. [1]

## Заключение

Разработанная модульная концепция обеспечивает воспроизводимый и экономически оправданный путь повышения киберустойчивости МСБ в условиях цифровой трансформации. Основные факторы успеха включают систематическую инвентаризацию активов, применение принципа минимальных привилегий, обязательное внедрение многофакторной аутентификации и проверяемые процедуры резервирования и восстановления. Пилотная реализация подтверждает, что даже при ограниченном бюджете МСБ могут достичь критического уровня защищённости, существенно снизив вероятность длительных простоев и репутационных потерь. Дальнейшие исследования целесообразно сосредоточить на адаптации модулей под отраслевые требования и экономическом моделировании возврата вложений в безопасность для типичных сегментов малого и среднего бизнеса. [1]

*Список литературы*

1. Абрамов В.И., Акулова Н.Л. – Цифровая трансформация экономики: учебное пособие. Москва: НИЯУ «МИФИ», 2020. – 77-91с.

2. ENISA. Good practices for SME cybersecurity м European Union Agency for Cybersecurity, руководства и рекомендации для малого и среднего бизнеса.