СНИЛ «Гандаль»
А. Д. Мицковец
БГЭУ (Минск)
*Научный руководитель — **А. В. Кармызов**, канд. экон. наук*

КИБЕРБЕЗОПАСНОСТЬ В ФИНАНСОВОМ СЕКТОРЕ: ВЫЗОВЫ СОВРЕМЕННОСТИ И ЛУЧШИЕ ПРАКТИКИ ЗАЩИТЫ

Современный финансовый сектор, переживая цифровую трансформацию, столкнулся с беспрецедентными киберугрозами. Будучи хранителями критически важных активов и данных, финансовые организации стали главной мишенью для киберпреступников. Новые вызовы требуют столь же динамичного развития и внедрения передовых практик защиты.

Одним из ключевых вызовов является рост изощренных целевых атак, таких как APT (Advanced Persistent Threat). В отличие от массовых рассылок эти атаки тщательно спланированы и нацелены на конкретные организации. Ярким примером является атака на Bangladesh Bank в 2016 г., когда злоумышленники, используя фишинговые письма и подобранные учетные данные, практически похитили 1 млрд долл. США через систему SWIFT [1].

Другим масштабным вызовом стало распространение программ-вымогателей (Ransomware), которые шифруют данные и парализуют работу учреждений. Атака на Colonial Pipeline в 2021 г. хоть и не была направлена на банк, наглядно показала, как кибератака может дестабилизировать критическую инфраструктуру, что напрямую касается и финансовой системы, где простой даже в течение нескольких часов означает колоссальные убытки и потерю доверия.

В ответ на эти угрозы финансовый сектор активно развивает и внедряет многоуровневую стратегию защиты. Одной из лучших практик является переход от периметровой защиты к модели Zero Trust (ZTA). Эта концепция, популяризированная аналитиками Forrester Research, предполагает принцип «никому не доверяй, проверяй всегда». Каждый запрос на доступ к системе или данным проверяется независимо от его источника, будь то внутри или вне корпоративной сети. Другой критически важной практикой является внедрение расширенной аутентификации и систем управления доступом. Стандартом де-факто становится многофакторная аутентификация (MFA), которая требует от пользователя предоставить как минимум два доказательства своей личности, например пароль и код из мобильного приложения. Более продвинутые организации внедряют биометрические методы, такие как отпечатки пальцев или распознавание лица [2].

Не менее важными являются постоянный мониторинг и оперативное реагирование. Создание центров безопасности (SOC — Security Operations Center) позволяет круглосуточно отслеживать события

безопасности, анализировать их с помощью систем SIEM (Security Information and Event Management) и немедленно реагировать на инциденты. Наконец, человеческий фактор остается самым слабым звеном, поэтому регулярное обучение и повышение осведомленности сотрудников являются обязательной практикой [3].

В заключение можно сказать, что постоянная гонка между злоумышленниками и защитниками требует не только инвестиций в передовые технологии, но и формирования целостной культуры безопасности, охватывающей процессы, людей и партнеров.

Источники

1. *Adebanjo, F.* Risk assessment on the case study of Bank of Bangladesh 2016 cyberattack / F. Adebanjo // Medium. — URL: https://medium.com/@fatimaosomo/risk-assessment-on-the-case-study-of-bank-of-bangladesh-2016-cyberattack-c88491b805cf (date of access: 26.10.2025).

2. *Upadhyay, V.* Why identity is the heart of Zero Trust — and how MFA, SSO, and Conditional Access secure it / V. Upadhyay // LinkedIn. — URL: https://www.linkedin.com/pulse/why-identity-heart-zero-trust-how-mfa-sso-conditional-vinay-upadhyay-cy1vf (date of access: 26.10.2025).

3. SOC & SIEM explained in cybersecurity // Medium. — URL: https://medium.com/@codedconversations/soc-siem-explained-in-cybersecurity-%EF%B8%8F-e5119d47e4ed (date of access: 26.10.2025).

И. А. Новик
БГЭУ (Минск)
Научный руководитель — ***А. В. Кармызов****, канд. экон. наук*

ЦИФРОВОЙ РАЗРЫВ МЕЖДУ ПОКОЛЕНИЯМИ КАК ВЫЗОВ ДЛЯ РАЗВИТИЯ СФЕРЫ УСЛУГ

Стремительная цифровизация социально-экономических процессов привела к усилению различий между поколениями в доступе к цифровым технологиям и навыках их использования. По определению исследователей, межпоколенческий цифровой разрыв — это неравенство в цифровых компетенциях и доступе к цифровым ресурсам между возрастными группами [1]. Эти различия напрямую влияют на качество и доступность услуг, так как современная сервисная инфраструктура активно переходит в цифровой формат.

Одним из наиболее заметных последствий является снижение доступности финансовых, медицинских и социальных услуг для пожилых людей. Как подчеркивает исследование BMC Health Services Research, низкая цифровая грамотность ограничивает использование услуг социального обслуживания [2]. В условиях, когда значительная