Маковий Максим Александрович
бакалавр, студент
Иваненко Ирина Анатольевна
канд. экон. наук, доцент

ГБОУВО РК «Крымский инженерно-педагогический
университет им. Февзи Якубова»
г. Симферополь, Республика Крым

КИБЕРБЕЗОПАСНОСТЬ В МЕЖДУНАРОДНОМ IT-БИЗНЕСЕ

Аннотация*: в условиях глобализации и цифровизации международного IT-бизнеса кибербезопасность становится ключевым фактором устойчивого развития компаний. Рост числа кибератак, ужесточение регуляторных требований и усиление конкуренции вынуждают организации внедрять комплексные меры защиты данных и инфраструктуры. В статье рассматриваются основные угрозы информационной безопасности в международном масштабе, такие как целевые атаки на корпоративные сети, утечки данных и государственный кибершпионаж.*

Ключевые слова*: кибербезопасность, международный IT-бизнес, кибератаки, защита данных, GDPR, искусственный интеллект, управление рисками.*

Современный глобальный IT-сектор сталкивается с усиливающимися рисками в цифровой сфере. Киберугрозы становятся все сложнее, а их последствия – серьезнее: от компрометации конфиденциальной информации до многомиллионных убытков и потери доверия клиентов. В этой ситуации защита от кибератак превращается не просто в техническую необходимость, а в стратегически важный аспект развития любой международной компании [1].

Ключевые риски для глобального IT-бизнеса.

1. Продвинутые целевые атаки (APT). Злоумышленники применяют сложные технологии для внедрения в корпоративные сети и скрытого сбора данных. Основными мишенями часто выступают крупные корпорации и госучреждения.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

2. Финансовое мошенничество и ransomware. Шифрование данных с последующим требованием выкупа остается одним из самых доходных направлений киберпреступности. По данным за 2023 год, мировой ущерб от таких атак превысил 20 млрд долл.

3. Утечки данных и нарушения GDPR. Ужесточение регуляций (например, GDPR в ЕС) делает защиту персональных данных критически важной. Штрафы за нарушения могут достигать 4% глобального оборота компании.

4. Уязвимости цепочек поставок (Supply Chain Attacks). Хакеры атакуют не только крупные компании, но и их поставщиков, используя слабые звенья в инфраструктуре.

5. Кибершпионаж и государственные угрозы. Международные конфликты усиливают риски цифрового шпионажа, особенно для компаний, работающих с критически важными технологиями [2].

В современном мире кибербезопасность стала одним из ключевых приоритетов для международного IT-бизнеса, поскольку цифровые угрозы постоянно эволюционируют и приобретают глобальный характер. Защита в киберпространстве требует комплексного подхода, учитывающего не только технологические аспекты, но и правовые, организационные и международные соглашения. Первым важным элементом стратегии является создание единых стандартов безопасности, которые могли бы применяться транснациональными корпорациями для обеспечения согласованного уровня защиты данных. Это включает в себя внедрение передовых технологий шифрования, многофакторной аутентификации и систем мониторинга угроз в реальном времени. Кроме того, необходимо развивать международное сотрудничество между государствами и частным сектором для оперативного обмена информацией о новых киберугрозах и уязвимостях. Важную роль играет также подготовка квалифицированных кадров, способных противостоять сложным атакам, что требует инвестиций в образование и обучение специалистов по всему миру [3].

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

В 2024–2025 годах отрасль кибербезопасности сталкивается с динамичными изменениями, вызванными ужесточением регулирования, технологическими прорывами и усложнением киберугроз.

1. Усиление регуляторного давления.

В ЕС вступила в силу директива NIS2, расширяющая требования к защите критической инфраструктуры, включая энергетику, транспорт и здравоохранение. Одновременно в ООН обсуждается глобальная киберрезолюция, которая может установить новые правила для борьбы с киберпреступностью. В США Комиссия по ценным бумагам и биржам (SEC) обязывает публичные компании раскрывать серьезные инциденты в течение 4 дней, что повышает прозрачность, но и увеличивает репутационные риски.

2. Атаки на цепочки поставок становятся масштабнее.

После громких взломов через сторонние сервисы (Okta, Microsoft, SolarWinds) компании активнее внедряют SBOM (Software Bill of Materials) – детализированный перечень компонентов ПО для выявления уязвимостей. Это помогает минимизировать риски, связанные с зависимостью от сторонних решений.

3. ИИ: инструмент защиты и новое оружие хакеров.

С одной стороны, защитные системы на основе ИИ (Darktrace, CrowdStrike) эффективно выявляют аномалии. С другой – злоумышленники используют Generative AI (WormGPT, FraudGPT) для создания убедительного фишинга, обхода CAPTCHA и автоматизации атак. Это делает киберугрозы более изощренными и массовыми.

4. Квантовая угроза: криптография под ударом.

Развитие квантовых вычислений ставит под вопрос надежность современных алгоритмов шифрования (RSA, ECC). В ответ NIST утвердил новые постквантовые криптографические стандарты, а технологические гиганты (Google, IBM, Cloudflare) уже тестируют устойчивые протоколы.

5. Эволюция ransomware: двойной шантаж и облачные атаки.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

Хакеры перешли к тактике double extortion, не только шифруя данные, но и угрожая их публикацией. Кроме того, с массовым переходом бизнеса в облака (AWS, Azure) злоумышленники все чаще атакуют облачные инфраструктуры, что требует усиления защиты на этом направлении.

Вывод: Кибербезопасность в международном IT-бизнесе является критически важным направлением, требующим глобального подхода и постоянной адаптации к новым угрозам. В условиях цифровизации и трансграничного характера кибератак компании сталкиваются с необходимостью внедрения комплексных стратегий защиты, включающих передовые технологии, международное сотрудничество и строгое соблюдение регуляторных требований. В будущем IT-компаниям придется учитывать такие вызовы, как развитие квантовых вычислений, использование AI злоумышленниками и ужесточение регуляций. Только благодаря продуманной, гибкой и международно-согласованной стратегии бизнес сможет минимизировать риски и обеспечить устойчивость в условиях растущих киберугроз. Глобальная кибербезопасность – это не просто технологическая задача, а непрерывный процесс, требующий совместных усилий всех участников цифровой экосистемы.

Список литературы

1. Гафнер В.В. Кибербезопасность в цифровой экономике: глобальные вызовы и стратегии защиты / В.В. Гафнер, С.В. Петров. – М.: Альпина Паблишер, 2023.

2. Луцкий В.А. Международные стандарты информационной безопасности: ISO 27001, NIST, GDPR / В.А. Луцкий, А.В. Шестаков. – СПб.: Питер, 2022.

3. Ермаков Д.Ю. Атаки на цепочки поставок: новые риски для международных IT-корпораций / Д.Ю. Ермаков // Информационная безопасность – 2023. – №4 – С. 45–52.

4. Смирнов А.А. Регуляторные тренды в кибербезопасности: NIS2 и их влияние на российский бизнес / А.А. Смирнов // Вопросы киберправа – 2024. – №1 – С. 12–25.

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

5. Иванова Е.К. ИИ в кибербезопасности: защита vs. угрозы / Е.К. Иванова // Цифровая экономика – 2023. – №3 – С. 78–89.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)