УДК 004.76:338.2

ЭКОНОМИЧЕСКИЕ ПОСЛЕДСТВИЯ КИБЕРАТАК

Жукова А.А., студентка гр. ЭКП-1-22, курс III
Научный руководитель: Уразбахтина Л.Р.
Казанский государственный энергетический университет, г. Казань, Россия

Современная цифровая трансформация привела к значительному увеличению зависимости мировых экономик от информационных технологий. Одновременно с этим возросли риски, связанные с киберугрозами, способными нанести ущерб как отдельным предприятиям, так и национальной инфраструктуре. В последние десятилетия кибератаки перестали быть изолированными инцидентами и стали системным вызовом, влияющим на финансовую стабильность, государственную безопасность и общественное доверие.

Кибератаки оказывают существенное влияние на экономическую систему. Финансовые потери могут включать прямые расходы, связанные с восстановлением работы, выплатами хакерам и штрафными санкциями. Нарушение работы предприятий приводит к значительным убыткам, особенно если атака затрагивает критически важные отрасли, такие как энергетика, логистика или здравоохранение. Дополнительный ущерб выражается в снижении доверия потребителей и инвесторов, поскольку публикация сведений о компрометации данных отрицательно сказывается на репутации компании. В условиях глобализированной экономики финансовые последствия атак распространяются далеко за пределы первоначального инцидента, затрагивая поставщиков, партнеров и клиентов.

Одним из наиболее известных примеров масштабных атак является случай с вирусом-вымогателем WannaCry, произошедший в 2017 году. Вредоносное программное обеспечение заразило более 200 000 компьютеров в 150 странах, вызвав сбои в работе как частных организаций, так и государственных учреждений. Среди пострадавших оказались Национальная служба здравоохранения Великобритании, испанская телекоммуникационная компания Telefónica и американская логистическая корпорация FedEx. Общий ущерб от атаки превысил 4 миллиарда долларов. Другой знаковый случай связан с атакой на Colonial Pipeline в 2021 году. Хакерская группа DarkSide проникла в сеть компании, что привело к временному прекращению поставок топлива на восточное побережье США. В результате американское правительство было вынуждено вмешаться в ситуацию, а организация потеряла миллионы долларов как из-за выкупа, выплаченного злоумышленникам, так и в связи с простоем производства [1].

За последний год в банковском секторе России также наблюдался значительный рост кибератак, что подтверждается данными Центра

кибербезопасности региона. Статистика свидетельствует об увеличении числа попыток несанкционированного доступа на 18 % в сравнении с предыдущим годом. АКБарс банк зафиксировал более 35 инцидентов, связанных с фишингом и вредоносными программами, при потенциальном ущербе в 12–15 миллионов рублей [2]. Сбербанк также сообщил о 28 случаях кибератак, что привело к кратковременным перебоям в работе онлайн-сервисов, а общий экономический ущерб банковской сферы вырос примерно на 20 % и оценивался в 250 миллионов рублей. Исследование, проведенное в марте 2024 года, установило, что 65 % инцидентов связаны с попытками кражи конфиденциальных данных, что подчеркивает растущую целенаправленность злоумышленников на финансовый сектор [3].

Малый и средний бизнес, обладая ограниченными ресурсами, оказывается особенно уязвим перед киберугрозами. Согласно исследованию IBM, средняя стоимость утечки данных в 2023 году составила 4,45 миллиона долларов. Для небольших компаний подобные убытки оказываются критическими и могут привести к банкротству. В отличие от крупных корпораций, обладающих специализированными отделами кибербезопасности, малые предприятия зачастую пренебрегают необходимыми мерами защиты, что делает их легкой мишенью для злоумышленников [4].

Государственные структуры, осознавая масштаб угроз, разрабатывают стратегии по минимизации последствий кибератак. Одним из ключевых направлений является повышение осведомленности сотрудников о потенциальных угрозах и проведение регулярных тренировок по реагированию на инциденты. Внедрение передовых технологий, включая искусственный интеллект и машинное обучение, позволяет автоматизировать процессы обнаружения атак и предотвращения утечек данных. Государственные регуляторы усиливают контроль над соблюдением стандартов кибербезопасности, требуя от организаций выполнения строгих норм защиты информации. Комплексный подход, сочетающий правовые, технические и организационные меры, является необходимым условием для снижения рисков и защиты критически важной инфраструктуры.

Анализ динамики киберугроз показывает, что банки демонстрируют высокую эффективность в оперативном обнаружении и нейтрализации атак благодаря современным технологиям мониторинга. Данные за последний год указывают на то, что крупные организации смогли сократить потенциальные потери за счет внедрения методов поведенческой аналитики, многофакторной аутентификации и регулярного обучения сотрудников. При этом сложность атак и стремительное развитие методов злоумышленников требуют дальнейших инвестиций в кибербезопасность. Результаты последних исследований подчеркивают необходимость активного сотрудничества между банками, государственными структурами и экспертами для формирования единых стандартов защиты, способных обеспечить финансовую стабильность в условиях растущей угрозы киберпреступности.

Вопрос кибербезопасности приобретает особую значимость в условиях растущей цифровизации экономики. Обострение конкуренции между государствами в сфере информационных технологий приводит к увеличению числа атак, организованных на государственном уровне. Кибершпионаж и дестабилизация цифровых систем становятся инструментами геополитической борьбы, что требует от национальных правительств разработки эффективных механизмов защиты. Экономические последствия подобных атак выражаются не только в прямых финансовых потерях, но и в снижении конкурентоспособности стран, потерях данных и угрозах национальной безопасности [5].

Развитие технологий неизбежно ведет к эволюции методов кибератак. Злоумышленники адаптируются к новым условиям, используя искусственный интеллект, автоматизированные системы и уязвимости в облачных сервисах. В ответ компании и правительства вынуждены инвестировать в инновационные методы защиты, включая поведенческую аналитику, многофакторную аутентификацию и блокчейн-технологии. Однако киберугрозы остаются динамичным явлением, требующим постоянного обновления стратегий защиты и усиления международного сотрудничества.

Современные исследования подтверждают, что игнорирование кибербезопасности может привести к катастрофическим последствиям. Отсутствие защиты информационных систем может не только подорвать устойчивость бизнеса, но и вызвать кризисы на национальном и глобальном уровнях. Внедрение комплексных мер, направленных на предотвращение атак и минимизацию их последствий, является необходимым условием для обеспечения устойчивости экономики в цифровую эпоху.

Список литературы:

1. Дацко, Т. Г. Влияние DDoS-атак на финансово-экономические результаты деятельности компаний / Т. Г. Дацко, И. Ф. Алешина // Научные исследования и разработки. Экономика. – 2017. – Т. 5, № 3. – С. 51-58.

2.Марцеленко, С. А. Оценка экономических последствий кибератак на региональные инфраструктуры // Актуальные вопросы современной экономики. – 2024. – № 8. – С. 297-302.

3. Малахов, С. Ю. Киберпреступность в России как угроза экономической безопасности // Обеспечение экономической безопасности России в современных условиях: Сборник научных трудов Всероссийской научной конференции - Москва: 2023. - С. 308-310.

4. Садыков, Р. С. Кибератаки как угроза экономической безопасности компаний и государственных структур / Р. С. Садыков // Тенденции развития науки и образования. – 2024. – № 105-5. – С. 98-101.

5. Арбатов, А.А. Экономическая безопасность России: Общий курс: учебник / Под ред. В.К. Сенчагова. - М.: БИНОМ. ЛЗ, 2018. - 815 с.