DOI: 10.58168/CISMP2024_311-313
УДК 004.56

АНАЛИЗ СОВРЕМЕННЫХ КИБЕРУГРОЗ, С КОТОРЫМИ СТАЛКИВАЮТСЯ ПРЕДПРИЯТИЯ ПРОМЫШЛЕННОГО КОМПЛЕКСА, И СТРАТЕГИИ ИХ МИНИМИЗАЦИИ

В.М. Дорошкевич, Г.Ш. Утешева, Аль-Судани Зайд Али Хуссейн

Кафедра КБ-1 «Защита информации», РТУ «МИРЭА», г. Москва

Аннотация: В статье рассмотрены современные киберугрозы, с которыми сталкивается промышленный комплекс, включая DDoS-атаки, фишинг, социальную инженерию, внедрение вредоносного ПО и несанкционированный доступ к информации. Проанализированы возможные экономические и репутационные потери от этих атак. Также предложены стратегии минимизации рисков.

Ключевые слова: промышленный комплекс, киберугрозы, DDoS-атаки, фишинг, вредоносное ПО, защита информации, минимизация рисков.

ANALYSIS OF MODERN CYBER THREATS FACED BY ENTERPRISES OF THE INDUSTRIAL COMPLEX AND STRATEGIES FOR THEIR MINIMIZATION

V.M. Doroshkevich, G.S. Utesheva, Al-Soudany Zaid Ali Hussein

Department of Information security, RTU MIREA, Moscow

Abstract: The article examines modern cyber threats faced by the industrial complex, including DDoS attacks, phishing, social engineering, malware injection and unauthorized access to information. The possible economic and reputational losses from these attacks are analyzed. Risk minimization strategies are also proposed.

Keywords: industrial complex, cyber threats, DDoS attacks, phishing, malware, information protection, risk minimization.

В последние годы промышленный комплекс стал одной из ключевых отраслей, активно использующих цифровые технологии для оптимизации процессов. Однако с увеличением цифровизации предприятия промышленного сектора сталкиваются с различными киберугрозами, которые могут нанести серьезный экономический и репутационный ущерб. В данной статье будут рассмотрены основные киберугрозы, с которыми сталкиваются компании промышленного комплекса, и предложения стратегии их минимизации.

В современном мире атаки на промышленные предприятия стали происходить чаще. Это связано с увеличением зависимости от цифровых технологий и глобальными геополитическими напряженностями. В таких условиях необходимо принять ряд мер для защиты предприятий

промышленного комплекса, чтобы не допустить нарушений в производстве и поставках продукции.

Причины атак на промышленный комплекс:

1. Экономические интересы. Атаки на промышленные предприятия часто направлены на дестабилизацию экономики. Успешная кибератака может привести к остановке производства, что создаст проблемы как на внутренних, так и на внешних рынках, негативно влияя на экономику страны.

2. Уязвимость инфраструктуры. Промышленный сектор включает сложные технологические цепочки, зависящие от стабильной работы различных систем. Атаки, направленные на разрушение инфраструктуры, могут привести к серьёзным последствиям: от остановки производства до возникновения аварийных ситуаций.

3. Технологические уязвимости. Злоумышленники нацеливаются на системы управления производственными процессами и программное обеспечение, используемое для мониторинга и анализа данных. В результате таких атак могут произойти сбои в производстве и логистике, что серьёзно повлияет на экономику предприятия.

Кибератаки на промышленный комплекс могут осуществляться различными методами. Далее рассмотрим несколько основных типов таких атак, их последствия и меры противодействия.

DDoS-атаки. Эти атаки направлены на перегрузку серверов и сетевой инфраструктуры, что приводит к недоступности сервисов. В промышленном комплексе это может затруднить работу систем управления и привести к сбоям в производственных процессах. Для защиты от DDoS-атак необходимо внедрять системы мониторинга трафика, позволяющие быстро реагировать на аномалии, а также применять фильтрацию трафика для блокировки подозрительных IP-адресов.

Фишинг и социальная инженерия. Эти атаки направлены на сотрудников компаний с целью получения их логинов и паролей к системам управления. Скомпрометированные данные могут привести к утечке коммерческой информации и производственных секретов. Для минимизации риска необходимо обучить персонал кибергигиене и использовать программное обеспечение для фильтрации подозрительных писем и ссылок.

Внедрение вредоносного ПО. При заражении системы вредоносным программным обеспечением злоумышленники получают доступ к конфиденциальной информации, включая финансовые данные, логины и пароли. В промышленном комплексе такие атаки могут привести к утечке производственных секретов и остановке работы оборудования. Для защиты следует использовать современные антивирусные программы и системы обнаружения вторжений, а также регулярно обучать сотрудников правилам безопасности.

Несанкционированный доступ к информации. Недовольные сотрудники могут использовать свои полномочия для получения доступа к конфиденциальной информации и её последующей продажи. Для

предотвращения подобных ситуаций необходимо ограничивать доступ к данным и проводить регулярные аудиты и мониторинг активности.

Выводы

В эпоху активной цифровизации промышленного комплекса киберугрозы становятся всё более актуальными. Фишинг, DDoS-атаки, вредоносное программное обеспечение и другие уязвимости представляют собой важные проблемы, требующие постоянного внимания. Для защиты предприятий необходимо внедрение современных систем кибербезопасности, регулярное обновление программного обеспечения, обучение сотрудников и создание резервных копий данных. Эти меры позволят значительно снизить риски, связанные с киберугрозами, и обеспечить стабильную работу промышленного сектора.

Список литературы

1. Иванова, Н.С. Цифровизация промышленности: перспективы и риски / Н.С. Иванова, А.В. Петренко // Вестник экономики и управления. – 2020. – № 5. – С. 34–45.

2. Сидоров, М.П. Технологические угрозы в цифровой экономике / М.П. Сидоров // Журнал информационной безопасности. – 2022. – Т. 12. – № 2. – С. 76–89.

3. Петров, К.И. Кибератаки в промышленности: меры предосторожности и способы защиты / К.И. Петров // Агентство кибербезопасности. – 2020. – С. 24–31.

References

1. Ivanova, N.S., Petrenko, A.V. Digitalization of Industry: Prospects and Risks / N.S. Ivanova, A.V. Petrenko // Journal of Economics and Management. – 2020. – № 5. – P. 34–45.

2. Sidorov, M.P. Technological Threats in the Digital Economy / M.P. Sidorov // Information Security Journal. – 2022. – Vol. 12. – № 2. – P. 76–89.

3. Petrov, K.I. Cyber Attacks in Industry: Precautionary Measures and Defense Methods / K.I. Petrov // Cybersecurity Agency. – 2020. – P. 24–31.