«РОЛЬ ГОСУДАРСТВЕННЫХ ОРГАНОВ В ПРОТИВОДЕЙСТВИИ КИБЕРУГРОЗАМ И ГИБРИДНЫМ АТАКАМ» / “THE ROLE OF GOVERNMENT AGENCIES IN COMBATING CYBER-THREATS AND HYBRID ATTACKS.”

Комилов Мехриддин Маликович
Курсант 2 курса военного факультета Б.Г.П.И.

Тема / Title

- Роль государственных органов в противодействии киберугрозам и гибридным атакам
- The Role of Government Agencies in Combating Cyber Threats and Hybrid Attacks

Ключевые слова / Keywords:

- кибербезопасность, гибридные атаки, государственные органы, киберугрозы, информационная безопасность, межведомственное взаимодействие
- cyber-security, hybrid attacks, government agencies, cyber threats, information security, inter-agency cooperation

Аннотация / Abstract: В условиях возрастающей цифровизации государственных сервисов и инфраструктуры государства, эффективность защиты от киберугроз и гибридных атак становится критической для национальной безопасности. Настоящая работа анализирует роль государственных органов в противодействии таким угрозам, включая функции мониторинга, раннего обнаружения, реагирования и восстановления. Рассматриваются различные типы атак (включая APT, фишинг, внедрение в цепочки поставок, манипуляции информацией) и особенности гибридных угроз, сочетающих технические, информационные и физические компоненты. Особое внимание уделено мерам организационного, правового и технического характера: выработке национальных стратегий кибербезопасности, межведомственному и публично-частному партнёрству, обмену разведданными, обучению кадров и цифровой грамотности общества. На основе международных исследований и практических кейсов даются рекомендации по укреплению роли государственных органов: улучшение координации, адаптация к развитию технологий (например, ИИ-угрозам), усиление нормативно-правовой базы и оперативное реагирование на инциденты. Работа указывает, что ключ к успеху — системный подход, объединяющий политику, технологии и человеческий фактор.

In the context of the increasing digitalization of government services and national infrastructure, the effectiveness of protection against cyber threats and hybrid attacks has become critical to national security. This study analyzes the role of government agencies in countering such threats, including their functions of monitoring, early

detection, response, and recovery. Various types of attacks are examined — including APTs, phishing, supply chain compromises, and information manipulation — as well as the distinctive features of hybrid threats that combine technical, informational, and physical components.

Special attention is given to organizational, legal, and technical measures: the development of national cybersecurity strategies, interagency and public-private partnerships, intelligence sharing, personnel training, and the enhancement of digital literacy across society. Based on international research and practical case studies, recommendations are provided to strengthen the role of government agencies: improving coordination, adapting to technological developments (e.g., AI-driven threats), reinforcing the regulatory framework, and ensuring rapid incident response. The study emphasizes that the key to success lies in a systemic approach that integrates policy, technology, and the human factor.

Основные разделы и содержание

Введение

Современная государственная деятельность всё более зависит от цифровых систем и инфраструктуры: информационные системы органов власти, сервисы для граждан, критическая инфраструктура. Это ведёт к росту уязвимости перед киберугрозами и гибридными атаками, которые часто исходят не только от одиночных хакеров, но и от организованных групп, государств-приступников и смешанных акторов (государство + преступность). Например, понятие «гибридной войны» в цифровой сфере рассматривается как сочетание кибератак, дезинформации и саботажа. (crimsonpublishers)

Государственные органы должны играть центральную роль в защите: как организаторы национальной стратегии, как координаторы между ведомствами и частным сектором, как исполнители (через CERT-службы, центры реагирования) и как правоприменители. Работы показывают, что без активного включения государства защита оказывается фрагментированной. (McKinsey & Company)

Типы угроз и гибридный характер

Исследования выделяют следующие типы кибератак, с которыми сталкиваются государственные органы: вредоносное ПО, DDoS-атаки, фишинг, внедрение в цепочки поставок (supply chain attacks), APT (Advanced Persistent Threats) и др. (proceedings.open.tudelft.nl)

Гибридные угрозы выходят за рамки чисто цифровых атак, сочетая, например, кибератаки с дезинформацией, манипуляцией общественным мнением и физическим саботажем инфраструктуры. Например, анализ указывает, что гибридные атаки на критическую инфраструктуру могут привести к серьёзным социальным, экономическим и экологическим последствиям. (MDPI)

В работе Tsaruk & Korniiets обсуждается парадигма «гибридной природы современных угроз» и её последствия для информационной безопасности. (scrd.eu)

Роль государственных органов: функции и механизмы

1. Стратегическое планирование и нормативная база.

Государство должно формировать национальные стратегии кибербезопасности, определять приоритеты, роли ведомств, модели финансирования и законодательную основу. (Amazonia Investiga)

2. Мониторинг, разведка и обмен информацией.

Органы должны осуществлять круглосуточный мониторинг угроз, собирать и анализировать данные об инцидентах и уязвимостях, формировать разведывательные продукты для этих целей. (McKinsey & Company)

3. Координация и межведомственное взаимодействие.

При серьёзных инцидентах вызывается участие разных ведомств (интеллектуальные службы, органы правопорядка, операторы инфраструктуры). Например, в США директива Presidential Policy Directive 41 (PPD-41) регулирует координацию федерального правительства при значительных киберинцидентах. (Википедия)

4. Публично-частное партнёрство и международное сотрудничество.

Государственные органы активно сотрудничают с частным сектором и другими странами для обмена разведданными, совместного реагирования и разработки стандартов. (McKinsey & Company)

5. Обучение, повышение осведомлённости и развитие кадров.

Цифровая грамотность, регулярные учения и тренинги позволяют повысить устойчивость к кибератакам. (Amazonia Investiga)

6. Реагирование и восстановление.

Органы власти должны иметь планы реагирования на инциденты, стандарты оценки тяжести инцидента, а также механизмы восстановления после атаки. (McKinsey & Company)

Проблемы и ограничения

- Юрисдикционные и международные ограничения: киберугрозы часто трансграничны, ведомственные рамки могут не охватывать весь спектр. (Scriptonet Analytics)
- Устаревшие технологии и инфраструктура в госорганах: увеличивают уязвимость. (IJSRP)
- Недостаточная координация и обмен информацией между ведомствами и с частным сектором. (Ijcat)
- Быстрое развитие технологий (например, ИИ-угроз), которое требует постоянной адаптации. (GSSSR Journal)

• Гибридный характер атак усложняет традиционные подходы: комбинация информационно-психологических, кибер и физико-технических методов. (crimsonpublishers)

Рекомендации

• Формирование единой точки отчёта об инцидентах и централизованного репозитория инцидентов. (McKinsey & Company)

• Разработка и внедрение стандарта оценки тяжести инцидента и плана мобилизации. (McKinsey & Company)

• Усиление общественно-частных партнёрств для обмена разведданными, совместных учений и разработки технологий.

• Постоянное обновление инфраструктуры и повышение цифровой грамотности среди госслужащих и граждан.

• Акцент на гибридах: введение стратегий, охватывающих не только технические, но и информационные, психологические и физические аспекты атак.

Заключение

Государственные органы играют ключевую роль в защите от киберугроз и гибридных атак. Однако для этого требуется не просто наличие ведомства, а системное, интегрированное и адаптивное управление: от стратегии до операций, от мониторинга до восстановления, и от национальных рамок до международного сотрудничества. Успех зависит от способности реагировать на быстро меняющуюся среду угроз, объединять технологии, политику и человеческий фактор. Обеспечение кибербезопасности — это не промежуточная задача, а непрерывный процесс в интересах национальной безопасности, экономики и общества.

СПИСОК ОСНОВНЫХ ИСТОЧНИКОВ:

1. Arbhi … Dimaz Cahya Ardhi, Dwi Puspita Sari, Benjamin Yankson, “Cyberattacks in government organizations: A systematic literature review of attack types and mitigation strategies.” Conference on Digital Government Research, 2025. (proceedings.open.tudelft.nl)

2. Tsaruk O., Korniiets M., “Hybrid nature of modern threats for cybersecurity and information security.” SCRD, 2023. (scrd.eu)

3. Beretas C., “Cyber Hybrid Warfare: Asymmetric Threat.” Research & Development in Material Science, 2020. (crimsonpublishers)

4. McKinsey & Company, “Follow the leaders: How governments can combat intensifying cybersecurity risks.” 2022. (McKinsey & Company)

5. “The role of government and law enforcement agencies in combating cybercrime.” Scriptonet. (Scriptonet Analytics)

6. Shostack A., Dykstra J., “Handling Pandemic-Scale Cyber Threats: Lessons from COVID-19.” 2024. (arXiv)

7. Schmitt M., Koutroumpis P., “Cyber Shadows: Neutralizing Security Threats with AI and Targeted Policy Measures.” 2025. (arXiv)

8. Information (MDPI), “Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era.” 2024. (MDPI)

9. MDPI, “Data Governance to Counter Hybrid Threats against Critical Infrastructures.” 2023. (MDPI)

10. International Journal of Advance Research, Ideas and Innovations in Technology, “Cyber security and government: safeguarding the public sectors in the digital era.” Smith O.Y., 2024. (IJARIIT)

11. International Journal of Computer Applications Technology and Research, “Roles and responsibilities in cybersecurity incident response.” 2025. (Ijcat)