Габорець Ольга Андріївна
доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету підготовки фахівців для підрозділів кримінальної поліції Донецького державного університету внутрішніх справ, доктор філософії, доцент

THE IMPACT OF CYBER THREATS ON COMMUNITY AND CITIZEN SECURITY: ANALYSIS AND PERSPECTIVES ON RESOLUTION

As we advance further into the 21st century, the integration of technology in daily life and government operations continues to expand. Alongside the benefits of this digital evolution, the rise in cyber threats poses a complex challenge to global security frameworks. These threats, ranging from personal data breaches to attacks on critical infrastructure, threaten not only the security of individuals but also the stability and functioning of entire communities.

The nature of cyber threats is intricate and multifaceted, involving various actors and techniques that evolve rapidly. Traditional security measures often fall short in the face of such dynamic and sophisticated threats. This paper seeks to dissect the implications of cyber threats on community and citizen security and to offer comprehensive strategies to effectively counter these risks.

Cyber threats manifest in various forms, each with unique impacts and challenges. Data breaches can expose personal information, leading to identity theft and financial fraud. Attacks on critical infrastructure, such as power grids or water supply systems, pose significant risks to public safety and can have catastrophic consequences for community life.

The economic implications of cyber threats are also profound. Businesses face potential financial losses due to downtime and the cost of recovering from cyber attacks, which can also damage consumer trust and brand reputation. At a broader level, the disruption of critical services can lead to economic instability within communities.

Strategically, the resolution of cyber threats necessitates a layered approach that includes technological, educational, and collaborative elements. Technologically, the deployment of advanced cybersecurity tools such as AI-driven threat detection systems and blockchain for enhancing data integrity is crucial. Educationally, increasing cyber awareness among citizens and training them in basic cyber hygiene practices are vital preventative measures.

Moreover, collaboration between government, industry, and academia is essential to foster a resilient cybersecurity framework. Such partnerships facilitate the sharing of best practices, drive the development of innovative security solutions, and ensure a unified response to cyber threats.

Cyber threats are a persistent and evolving challenge that significantly impacts community and citizen security. Addressing these threats requires a holistic approach that integrates advanced technological solutions, educative initiatives, and strategic collaborations. By fostering a culture of cyber resilience and adopting comprehensive protective measures, communities can enhance their defenses against the increasingly sophisticated landscape of cyber threats, thereby securing the digital and physical well-

being of their citizens.

Габорець Ольга Андріївна
доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету підготовки фахівців для підрозділів кримінальної поліції Донецького державного університету внутрішніх справ, доктор філософії, доцент
Шаєц Єлизавета Олександрівна
курсантка 2-го курсу факультету підготовки фахівців для підрозділів кримінальної поліції Донецького державного університету внутрішніх справ, рядова поліції

АНАЛІЗ КІБЕРЗАГРОЗ ДЛЯ ГРОМАДСЬКИХ СТРУКТУР: ВИКЛИКИ ТА МОЖЛИВОСТІ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ

У контексті глобалізованого інформаційного суспільства, зростання залежності від цифрових технологій веде до збільшення кібернетичних ризиків, особливо для громадських структур. Ці структури, характеризуючись високим рівнем доступності та обмеженими ресурсами для кіберзахисту, є вразливими до широкого спектру кібернетичних загроз, включаючи малварні атаки, фішинг, а також комплексні загрози, як-от розподілені атаки на відмову у обслуговуванні (DDoS).

Протидія цим загрозам вимагає розробки інтегрованих стратегій кіберрезилієнтності, які включають не лише технічні рішення, але й адаптацію організаційних політик і процедур. Ефективне впровадження політик безпеки, аудити вразливостей, а також застосування принципів мінімальних привілеїв і багаторівневої захисту є ключовими для захисту від потенційних кіберзагроз.

Одночасно, зазначені виклики стимулюють інноваційні підходи у сфері кібербезпеки, зокрема використання алгоритмів машинного навчання та штучного інтелекту для аналізу поведінки мережі та ідентифікації аномалій. Впровадження кіберінтелігенції та прогностичних аналітичних інструментів може забезпечити більш проактивний підхід до розпізнавання та нейтралізації загроз.

Оцінка сучасного кіберсередовища вимагає врахування зростаючої інтеграції кіберфізичних систем в повсякденні аспекти громадського управління, що ставить під загрозу не тільки інформаційні ресурси, але й фізичну інфраструктуру. Завдяки технологічному прогресу кібератаки стають більш складними і витонченими, що зумовлює потребу в постійному оновленні кіберзахисних технологій та методик. Значна увага в цьому контексті приділяється криптографічному захисту даних, розробці безпечних комунікаційних протоколів і підвищенню рівня кібергігієни серед користувачів.

З іншого боку, важливим аспектом забезпечення кібербезпеки є розвиток міжнародної співпраці та розробка глобальних норм і стандартів. Це передбачає не лише узгодження технічних вимог, але й консолідацію правових та етичних