В.З. Хаимов,
Всероссийский научно-исследовательский институт
документоведения и архивного дела (ВНИИДАД),
ведущий научный сотрудник, кандидат технических наук

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ХРАНЕНИИ И ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

(в рамках темы 3.1 НИОКР ВНИИДАД «Исследование и анализ зарубежной периодической литературы, материалов официальных интернет-сайтов, конференций, международных научных проектов по проблемам управления электронными документами и внедрения современных информационных технологий в делопроизводство и архивное дело»)

Аннотация: Констатируется, что XXI век стал рубежным для создания и активного развития мер по обеспечению непрерывного контроля защищенности, предупреждения, выявления и реагирования на инциденты информационной безопасности действующих и создающихся центров обработки данных и хранения электронных документов (*ЭД*). В связи с этим обращается внимание на *Постановление Правительства РФ от 2 марта 2022 г. N 279 «О государственной информационной системе "Платформа "Центр хранения электронных документов"», в котором,* наряду с требованиями об обеспечении сохранности, аутентичности, целостности и пригодности для использования на протяжении всего срока хранения подлинников архивных документов в электронном виде, указывается на **необходимость защиты информации от несанкционированного доступа**, копирования, искажения, удаления или блокирования доступа к ней, а также от иных неправомерных действий. В этих условиях становится общепризнанной целесообразность производства указанных действий в рамках организуемых в разных странах, в том числе и в России, Центров управления безопасностью *SOC* (*The Security Operation Center, SOC*) – структур для управления и повышения общей безопасности организации путем обнаружения, анализа и реагирования на угрозы и инциденты

кибербезопасности с использованием **людей, процессов, технологий, управления и соответствия требованиям** (*People, Processes and Technologies, Governance and Compliance PPTGC*).

Приводятся сведения о возможных архитектурных подходах к построению *SOC*, о разновидностях их операционных моделей, о факторах, влияющих на выбор операционной модели *SOC.* Достаточно подробно анализируется роль каждого из компонентов структуры *PPTGC*. Дается понятие об используемых для поддержания стратегических решений, обеспечения качества и получения тактического контроля деятельности *SOC* количественных показателей – типовых метрик.

Обращается внимание также на сложившуюся к настоящему времени практику существования Центров управления сетью *NOC* (*The network operating center*), обеспечивающих работоспособность и доступность активов информационных технологий, которые функционируют независимо от Центров управления безопасностью *SOC*, направленных на безопасность собственно *ИТ*-активов, в том числе сохраняемых и используемых электронных документов, и защиту их от кибератак. Констатируется, что де-факто Центры *NOC* и *SOC* работают разрозненно, не координируя свою деятельность друг с другом, что снижает эффективность работы обеих структур. На этом фоне, на основании широкого и глубокого обсуждения, делается вывод о крайне важности реорганизации эти разрозненных структур и объединении их в **единое интегрированное подразделение**, чтобы эффективно противостоять кибератакам, угрозам и вандализму, обеспечивая при этом снижение общих эксплуатационных расходов. Подчеркивается, что комплексный интеграционный подход прокладывает путь к мощному синергизму между *NOC* и *SOC* через структуру *PPTGC* в многоуровневом мониторинге и реагировании на инциденты.

Обсуждаются варианты построения предлагаемых рядом авторов **интегрированных *NOC и SOC*.** Оцениваются достигаемые преимущества от организации таких структур. Приводятся сведения о вызовах, которые могут

встретиться при разработках и последующем функционировании интегрированных *NOC* и *SOC*.

Ключевые слова: инциденты информационной безопасности, центры управления безопасностью, центры управления сетью, управление инцидентами, анализ угроз, операционные модели, программное обеспечение безопасности.

METHODS FOR COUNTERING INFORMATION SECURITY THREATS IN THE STORAGE AND USE OF ELECTRONIC DOCUMENTS

Abstract: The necessity of ensuring continuous monitoring of security, prevention, detection and response to information security incidents in modern data processing centers and storage of electronic documents is substantiated. The relevance of creating SOC information security control centers is noted, the ideology, principles of their organization and activities are revealed. SOCs are cited as bringing together processes, technology, and people to manage and enhance an organization's overall security through situational awareness, risk mitigation, and compliance. It also describes integrated information security control centers that ensure the coordinated operation of SOCs with existing network control centers NOC. The expediency of combining them into a single integrated unit is emphasized to effectively counter cyber attacks, threats, vandalism and, at the same time, to reduce overall operating costs.

Keywords: information security incidents, security control centers, network control centers, incident management, threat analysis, operating models, security software.