Об организации национальной системы кибербезопасности в США

Романовский А. Р., магистр. БГУ,
науч. рук. проф. Свилас С. Ф., д-р ист. наук, доц.

Организация системы кибербезопасности в Соединенных Штатах Америки носит комплексный многоуровневый характер.

В структуре органов, отвечающих за кибербезопасность в США, ключевые роли играют Белый дом, Министерство внутренней безопасности, Министерство обороны, Агентство национальной безопасности, Министерство юстиции, Федеральное бюро расследований, отраслевые агентства, другие федеральные и государственные органы, местные и территориальные правительства, а также частный и неправительственный сектора. В США все федеральные департаменты и агентства отвечают за защиту своих собственных систем ИКТ, а многие из них имеют отраслевые обязанности в отношении критической инфраструктуры [1].

Несмотря на то, что координация мер реагирования на кризисы осуществляется федеральным правительством централизованно, их исполнение децентрализовано. При этом главную координирующую роль на национальном уровне в киберсфере играет Межведомственный комитет по политике в области информационно-коммуникационной инфраструктуры (МКП-ИКИ) Совета национальной безопасности (СНБ) США.

Министерство внутренней безопасности (МВБ) координирует общие федеральные усилия по защите критической инфраструктуры, включая укрепление ее безопасности и устойчивости, помощь федеральным гражданским агентствам в разработке и реализации политики, реагировании на инциденты и др. Алгоритм действий, роли и обязанности различных игроков прописаны в руководящем документе МВБ – Национальном плане реагирования на кибер-инциденты [2].

Действующее в рамках МВБ Управление национальной защиты и программ (УНЗП) отвечает за поддержание безопасности критической инфраструктуры. УНЗП включает Национальный центр интеграции кибербезопасности и коммуникаций (НЦИКБК), обеспечивающий сотрудничество и обмен информацией между всеми уровнями правительства и частным сектором и предоставляющий информацию об уязвимостях, вторжениях, инцидентах и действиях по восстановлению данных.

В свою очередь, в состав НЦИКБК входят такие подразделения, как Компьютерная команда экстренной готовности США (US Computer Emergency Readiness Team, US-CERT), Компьютерная команда экстренной готовности в промышленных системах управления (Industrial Control Systems Cyber Emergency Response Team, ICS-CERT) и Национальный координационный

центр коммуникаций (National Coordinating Centre for Communications, NCC). Эти подразделения обеспечивают основу для координации и поддержки всех федеральных агентств в обеспечении безопасности их систем и помощи в решении любых вопросов, связанных с кибербезопасностью [3].

Основным федеральным межведомственным механизмом, координирующим подготовку, реагирование, восстановление и обмен оперативной информацией во время национально значимых киберинцидентов, является Национальная координационная группа киберреагирования (NCRCG). В ее состав входят представители 19 федеральных министерств и ведомств, которые координируют свою деятельность с местными органами власти и частным сектором [2].

В США обмен информацией об оценке уязвимостей и рисков между федеральным правительством и частным сектором является добровольным. Основная ответственность за защиту, реагирование и восстановление после кибератак, направленных на критическую инфраструктуру, лежит на владельцах и операторах этих активов. Политика правительства США направлена на расширение обмена информацией с частным сектором.

Литература

1. Pernik, P. National Cyber Security Organisation: United States [Electronic resource] / P. Pernik // CCDCOE. – Tallinn, 2016. – Mode of access: https://ccdcoe.org/uploads/2018/10/CS_organisation_USA_122015.pdf. – Date of access: 22.02.2022.

2. National Cyber Incident Response Plan / U.S. Department of Homeland Security [Electronic resource]. – December 2016. – Mode of access: https://www.cisa.gov/uscert/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf. – Date of access: 06.03.2022.

3. Federal information security management act of 2002 [Electronic resource] // Library of Congress. – Mode of access: https://www.congress.gov/bill/107th-congress/house-bill/3844. – Date of access: 22.02.2022.

«Белая Русь» в западноевропейских источниках Средневековья: историография вопроса

Румчик И. Н., асп. I к. БГУ,
науч. рук. Прохоров А. А., канд. ист. наук, доц.

Целью данной статьи является обзор и краткая характеристика работ, посвященных исследованию названия «Белая Русь» в западноевропейских средневековых источниках. В силу данного обстоятельства в статье не будут рассматриваться обширные работы, посвященные Белой Руси в источниках Великого Княжества Литовского, Московского княжества, а также труды,