Научная статья
УДК 004.056

СРАВНЕНИЕ ПОДХОДОВ К РАССЛЕДОВАНИЮ КИБЕР ИНЦИДЕНТОВ В РОССИИ И ЗАРУБЕЖНЫХ СТРАНАХ

А.К. Макарова[1,*], Н.А. Макеев[1]

[1] Санкт-Петербургский государственный университет телекоммуникаций имени профессора М.А. Бонч-Бруевича, Санкт-Петербург, Россия
[*]E-mail: Alex-ecureuil@mail.ru

Аннотация. Данная работа посвящена исследованию в области расследования киберинцидентов КИИ в Российской Федерации и зарубежных странах на примере Соединённых Штатов Америки. Рассмотрено функционирование систем защиты от киберугроз и подходы, применяемые при их расследовании. Произведен сравнительный анализ параметров обеспечения безопасности объектов КИИ, методов расследования киберинцидентов и реагирования на них. В результате исследования предложены общие рекомендации по внедрению подходов к расследованию инцидентов на объектах КИИ.

Ключевые слова: защита информации; критическая инфраструктура; информационная безопасность; сравнительный анализ.

Для цитирования: Макарова А.К., Макеев Н.А. Сравнение подходов к расследованию кибер инцидентов в России и зарубежных странах// Вестник науки и образования Северо-Запада России. 2023. Т.9, №3. С. 84–89.

Original article

COMPARISON OF APPROACHES TO THE INVESTIGATION OF CYBER INCIDENTS IN RUSSIA AND FOREIGN COUNTRIES

A.K. Makarova[1,*], N.A. Makeev[1]

[1] St. Petersburg State University of Telecommunications named after Professor M.A. Bonch-Bruevich, Sankt-Petersburg, Russia,
[*]E-mail: Alex-ecureuil@mail.ru

Abstract. This work is devoted to research in the field of investigation of cyber incidents of CII in the Russian Federation and foreign countries on the example of the United States of America. The functioning of protection systems against cyber threats and approaches used in their investigation are considered. A comparative analysis of the parameters for ensuring the security of CII facilities, methods for investigating cyber incidents and responding to them was made. As a result of the study, general recommendations were proposed for the implementation of approaches to the investigation of incidents at CII facilities.

Key words: information security; critical infrastructure; Information Security; comparative analysis.

For citation: Makarova A.K., Makeev N.A. Comparison of approaches to the investigation of cyber incidents in Russia and foreign countries. *Journal of Science and Education of North-West Russia*. 2023. Vol. 9, No. 3, pp. 84–89.

Введение

Защита критической информационной инфраструктуры (КИИ) является актуальнейшей темой, как для представителей государства, так и для специалистов по информационной безопасности (ИБ). Данные и процессы обрабатываемые в системах КИИ представляет огромный интерес для хакеров, а нападения могут привести к сбою предоставления услуг, остановке производств, утечке конфиденциальных данных или даже угрожать жизни и безопасности людей. Не менее важными являются действия по своевременному реагированию на инциденты и их локализация, в целях сохранения работоспособности системы и избежание возможных будущих угроз.

Из всего выше сказанного следует единственный верный подход, а именно, необходимость учета опыта защиты и расследования инцидентов в области КИИ не только в РФ, но и в других, близких по уровню развития странах, для единого понимания сущности расследования кибер-инцидентов КИИ. Для начального сравнения выбрана США, в силу развитой технологической отрасли, можно сказать, что она является передовой в области ИБ. При этом стоит отметить, что КИИ в том понимании в каком оно существует в России, в США нету. Нас интересует сама система защиты критически важных для страны объектов, а она есть.

В рамках данной работы будут проанализированы и описаны ключевые отличия в процессах реагирования на инциденты в РФ и США, а также рассмотрим основные методы, применяемые при расследовании инцидентов на объекты КИИ. Так же, в дальнейшем, к сравнению можно подключить и другие страны, например Китай.

Результаты анализа

Расследование инцидентов на субъектах КИИ в России выполняется различными государственными ведомствами, такими как Федеральная служба безопасности (ФСБ), Федеральная служба по техническому и экспортному контролю (ФСТЭК), Министерство внутренних дел (МВД) и др. [1].

Все субъекты КИИ в обязательном порядке подключаются к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) на информационные ресурсы РФ [2]. Информация из ГосСОПКА передается в национальный координационный центр по компьютерным инцидентам (НКЦКИ), который принимает непосредственное участие в обнаружении, предупреждении и ликвидации последствий кибератак (рисунок 1).

Рисунок 1 – Схема функционирование системы защиты КИИ в РФ

Помимо координации действий, контроля защищенности и расследования инцидентов на объектах КИИ, ГосСОПКА прогнозирует ситуации в области информационной безопасности России.

В США существует множество центров обмена информацией, которые собирают полученную информацию об угрозах и затем предоставляют эту информацию своим партнерам. Центры делятся на местные и региональные, национальные, следственные и партнеров [3].

Расследование инцидентов на субъектах КИИ в США, происходит в соответствии с президентской политической директивой под названием "Координация и реагирование на киберинциденты" или (PPD)/PPD-41. Она устанавливает принципы и структуру для координации реагирования на киберугрозы на федеральном уровне в США [4]. В процессе реагирования и расследования участвуют такие структуры как, Федеральное бюро расследований (ФБР) и Министерством внутренней безопасности (DHS), Национальный центр кибербезопасности и коммуникаций (NCCIC), Межагентственный комитет по кибербезопасности и координации (IPCC), Государственные и местные органы безопасности, общественно-частное партнерство [5]. Ниже в тексте представлена схема их функционирования (Рисунок 2).

Рисунок 2 – Схема функционирование системы защиты КИИ в США

Все критические информационные объекты национального масштаба подключаются к системе защиты, известной как Национальная система защиты критической информационной инфраструктуры (National Critical Infrastructure Protection System, NCIPS). NCIPS играет ключевую роль в координации и обмене информацией о кибербезопасности между различными органами и структурами в США [6]. Эта система направлена на предотвращение, обнаружение, реагирование и восстановление от киберинцидентов на КИИ в стране.

Для понимания различий в реагировании на инциденты в РФ и США на объектах, принадлежащих к критической инфраструктуре, может отличаться по нескольким

ISSN 2413–9858

параметрам. Сравнение по параметрам для наглядности различий представлено в табличном виде (Таблица1).

Таблица 1 – Параметры различия реагирования

Параметры	РФ	США
Степень централизации	Централизованная система управления КИИ	Децентрализованная система управления КИИ
Центр координации	Национальный центр координации (НЦК). Единый центр, к которому подключаются все объекты КИИ.	National Cybersecurity and Communications Integration Center (NCCIC), National Infrastructure Protection Plan (NIPP) Supplemental Tool on connecting to the National Infrastructure Coordinating Center (NICC).
Система координации	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).	Cybersecurity and Infrastructure Security Agency (CISA) Central.
Уровень координации	Сотрудничество с частным сектором и другими госструктурами.	Развитое сотрудничество между частным сектором и государственными агентствами, информационный обмен, совместные учения.
Способности и ресурсы	Отечественные технические разработки, собственный технический ресурс и инструменты для обнаружения и реагирования на инциденты в КИИ.	Современные технические средства, финансирование и доступ к передовым технологиям и инструментам для обнаружения и реагирования на инциденты.
Масштабы объектов КИИ	Широкий спектр объектов, включая энергетические системы, транспортную инфраструктуру, банковские системы и другие критически важные секторы.	Система разделена на критические инфраструктурные секторы, каждый из которых отвечает за защиту своей отрасли.

В результате, можно сказать, что корневые различия заключаются в построении системы защиты на уровне законодательства и построения структуры организаций реагирования на инциденты, связанные с КИИ. Так, сотрудничество и координация является главным отличием. Так же можно отметить разницу в развитие технических средств и систем, применяемых на объектах КИИ [7]. При этом, такие методы как форензика, анализ логов, SIEM системы и инструменты криминалистики являются общепринятыми методами по расследованию инцидентов КИИ. Методы могут различаться, например, в развитие программного обеспечения, используемого для их реализации.

Выводы

Была проанализирована структура построения системы реагирования и дальнейшего расследования инцидентов КИИ, выделены параметры сравнения: степень централизации, центр координации, система координации, уровень координации, способности и ресурсы,

масштабы объектов КИИ. Произведен сравнительный анализ параметров реагирования на инциденты КИИ В РФ и США.

Получены схемы построения структур организации защиты КИИ, сравнительные параметры и вывод о эффективности реализуемой в РФ структуры реагирования на инциденты КИИ. Итогом является вывод, о том, такие методы как форензика, анализ логов, SIEM системы и инструменты криминалистики являются общепринятыми методами по расследованию инцидентов КИИ. Определенно важной частью расследования инцидентов КИИ является сотрудничество и координация между различными структурами и организациями, включая правоохранительные органы, государственные службы и частные компании. Это позволяет объединить ресурсы, обменять информацией и координировать действия в целях эффективного расследования и предотвращения будущих инцидентов.

В дальнейшем планируется более детализированное сравнение, экспериментально-теоретическая корректировка нашего КИИ на основании сравнительной таблицы и мнения экспертов по ней.

СПИСОК ИСТОЧНИКОВ

1. Кузнецов С.А., Куликов И.А., Фоминых А.А. Сравнение КИИ и методов категорирования КИИ в РФ и США // Актуальные научные исследования в современном мире. 2021. № 6-1(74). С. 63-68.

2. Типовые офтальмологические информационные системы, являющиеся объектами критической информационной инфраструктуры / Красов А.В., Лансере Н.Н., Фадеев И.И., Гельфанд А.М., Лесневский М.В. // Офтальмохирургия. 2022. № S4. С. 85-91.

3. Степаненко С.И. ГосСОПКА в области критической информационной инфраструктуры Российской Федерации // The World of Science Without Borders. 2022 года, №2. С. 348-350.

4. Организация концептуальной модели критической информационной инфраструктуры / А. М. Гельфанд, Н. Н. Лансере, А. А. Ложкина, И. И. Фадеев // Методы и технические средства обеспечения безопасности информации. 2020. № 29. С. 39-40.

5. Абдуллин Т.И., Баев В.Д., Буйневич М.В., Бурзунов Д.Д., Васильева И.Н., Галиуллина Э.Ф. и др. Цифровые технологии и проблемы информационной безопасности: монография. СПб: СПГЭУ 2021. 163 с.

6. Миняев А.А., Красов А.В., методика оценки эффективности системы защиты информации территориально-распределенных информационных систем // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 3. С. 26-32.

7. Лансере Н.Н. Внедрение методологии быстрой оценки объектов критическая инфраструктуры для учреждений образования // Управление образованием: теория и практика. 2022. № 2(48). С. 10-16.

REFERENCES

1. Kuznecov S.A., Kulikov I.A., Fominyh A.A. *Sravnenie KII i metodov kategorirovaniya KII v RF i SShA* [Comparison of CII and CII categorization methods in the Russian Federation and the USA]. *Aktual'nye nauchnye issledovaniya v sovremennom mire*. 2021. No. 6-1(74), pp. 63-68.

2. Krasov A.V., Lansere N.N., Fadeev I.I., Gelfand A.M., Lesnevsky M.V. *Tipovye oftal'mologicheskie informacionnye sistemy, yavlyayushchiesya ob"ektami kriticheskoj*

informacionnoj infrastruktury [Typical ophthalmological information systems that are objects of critical information infrastructure]. *Oftal'mohirurgiya.* 2022. No. S4, pp. 85-91.

3. Stepanenko, S. I. *GosSOPKA v oblasti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii* [GosSOPKA in the field of critical information infrastructure of the Russian Federation]. The World of Science Without Borders. 2022. No.2, pp. 348-350.

4. Gelfand A. M., Lancere N. N., Lozhkina A. A., Fadeev I. I. *Organizaciya konceptual'noj modeli kriticheskoj informacionnoj infrastruktury* [Organization of a conceptual model of critical information infrastructure]. *Metody i tekhnicheskie sredstva obespecheniya bezopasnosti informacii*. 2020. No. 29, pp. 39-40.

5. Abdullin T.I., Baev V.D., Buynevich M.V., Burzunov D.D., Vasil'eva I.N., Galiullina E.F. and others. *Cifrovye tekhnologii i problemy informacionnoj bezopasnosti: monografiya* [Digital technologies and problems of information security: monograph]. SPb: SPGEU, 2021. 163 p.

6. Minyaev A.A., Krasov A.V. *Metodika ocenki effektivnosti sistemy zashchity informacii territorial'no-raspredelennyh informacionnyh sistem* [Methodology for evaluating the effectiveness of the information security system of geographically distributed information systems]. *Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta tekhnologii i dizajna. Seriya 1: Estestvennye i tekhnicheskie nauki*. 2020. No. 3, pp. 26-32.

7. Lancere, N. N. *Vnedrenie metodologii bystroj ocenki ob"ektov kriticheskaya infrastruktury dlya uchrezhdenij obrazovaniya* [Implementation of the methodology for rapid assessment of critical infrastructure objects for educational institutions]. *Upravlenie obrazovaniem: teoriya i praktika*. 2022. No. 2(48), pp. 10-16.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Макарова Александра Константиновна – студент института магистратуры, Санкт-Петербургский государственный университет телекоммуникаций имени профессора М. А. Бонч-Бруевича (Россия, 193232, Санкт-Петербург, пр. Большевиков д.22, к.1, e-mail: Alex-ecureuil@mail.ru).

Макеев Никита Андреевич – студент института магистратуры, Санкт-Петербургский государственный университет телекоммуникаций имени профессора М. А. Бонч-Бруевича (Россия, 193232, Санкт-Петербург, пр. Большевиков д.22, к.1, e-mail: nikita.makeev.2000@gmail.com).

INFORMATION ABOUT THE AUTHORS

Makarova Alexandra Konstantinovna – student of the Master's Institute, St. Petersburg State University of Telecommunications named after Professor M.A. Bonch-Bruevich (Russia, 193232, St. Petersburg, Bolshevikov Ave. 22, building 1, e-mail: Alex-ecureuil@mail.ru)
).

Makeev Nikita Andreevich – student of the Master's Institute, St. Petersburg State University of Telecommunications named after Professor M.A. Bonch-Bruevich (Russia, 193232, St. Petersburg, Bolshevikov Ave. 22, building 1, e-mail: nikita.makeev.2000@gmail.com).

Статья поступила в редакцию 09.09.2023; одобрена после рецензирования 20.09.2023, принята к публикации 25.09.2023.
The article was submitted 09.09.2023; approved after reviewing 20.09.2023; accepted for publication 25.09.2023.