БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2022. – № 4 (107). – 39–51

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

УДК 004 DOI: 10.17212/2782-2230-2022-4-39-51

ПРАКТИКА СОЗДАНИЯ ЦЕНТРА МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

А.А. КИСЕЛЕВ[1], И.В. КОРОТКИХ[2], В.В. ШОТТ[3]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры защиты информации. E-mail: anton.kiselev@corp.nstu.ru*
[2] *630008, г. Новосибирск, ул. Бориса Богаткова, 63/1, ООО «Системы информационной безопасности», начальник Центра мониторинга информационных систем. E-mail: kiv@sib-nsk.net*
[3] *127015, РФ, г. Москва, Большая Новодмитровская, 14/1, ООО «Инфосистем Джет», аналитик. E-mail: shottvv@mail.ru*

Интенсивно меняющийся ландшафт угроз безопасности информации, связанный напрямую с развитием информационных технологий, требует непрерывного автоматизированного контроля событий информационной безопасности с целью оперативного реагирования, ретроспективного анализа на предмет таргетированных атак, а также выполнения требований регуляторов сферы. В настоящей статье представлен процесс создания внедряемой повсеместно концепции – Центра мониторинга информационной безопасности. Этот сложный, многофакторный процесс учитывает проработку нормативно-правовых актов и нормативно-методической документации, анализ актуальных международных практик, формирование пула используемых технологий, формирование команды обслуживания и отладку рабочих процессов. При этом должны учитываться возможность взаимодействия Центра с регулирующими органами, особенностями коммуникации с заказчиками, собственная устойчивость к атакам, экономическая целесообразность, особенности человеческой психологии и тому подобное. Для визуализации работы Центра представлена процессная схема его работы. В статье уделено внимание выбору ядра Центра – SIEM-системы. Результат наглядно представляет текущий срез российского рынка систем такого класса, что важно в контексте импортозамещения.

Ключевые слова: SOC, Центр мониторинга информационной безопасности, мониторинг информационной безопасности, компьютерный инцидент, компьютерная атака, ГосСОПКА, SIEM

* Статья получена 21 октября 2022 г.

ВВЕДЕНИЕ

Растущий поток примеров инцидентов информационной безопасности (ИБ) подтверждают актуальность необходимости совершенствования применяемого инструментария. Обусловлено это факторами, связанными и с развитием самой сферы ИТ, «размытием» периметра безопасности, а также ростом зависимости уровня информационной безопасности от лояльности буквально каждого сотрудника, имеющего доступ к чувствительной информации организации. В качестве одного из основных решений проблем в статье рассматривается Центр мониторинга информационной безопасности (Центр), где в непрерывном режиме осуществляется сбор, обработка/анализ всей информации, свидетельствующей о происходящих процессах в устройствах сети или информационной системы, с помощью агентов системы мониторинга Центра. Качественный анализ позволяет как своевременно распознать и среагировать на компьютерную атаку (КА), так и расследовать компьютерный инцидент (КИ). Для обозначения таких Центров используется аббревиатура SOC, а в России используется обозначение – центр ГосСОПКА. Под этим термином понимается единый территориально распределенный комплекс, включающий «силы» и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты [1].

Авторами преследовалась цель проведения обзора, анализа источников, и формирования рекомендации по выбору SIEM систем.

1. МЕТОДИКА РАЗРАБОТКИ ЦЕНТРА МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В отсутствие единого подхода к разработке и реализации Центра заинтересованные компании идут непростым путем интеграции лучших практик, как правило международных, с требованиями отечественного законодательства.

В соответствии с Указом Президента РФ от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [2] федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования центров ГосСОПКА, была назначена Федеральная служба безопасности Российской Федерации (далее – ФСБ России). Приказом ФСБ России от 24.07.2018 № 366 в структуре ФСБ России был выделен отдельный орган, обеспечивающий координацию деятельности по данному направлению обеспечения информационной безопасности нашего государства. Данный орган имеет соответствующее наименование – Нацио-

нальный координационный центр по компьютерным инцидентам (далее – НКЦКИ).

НКЦКИ разработал методические рекомендации, которыми необходимо руководствоваться при создании центров ГосСОПКА:

- методические рекомендации по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации [3];
- методические рекомендации по обнаружению компьютерных атак на информационные ресурсы Российской Федерации;
- методические рекомендации по проведению мероприятий по оценке степени защищенности от компьютерных атак;
- методические рекомендации по установлению причин и ликвидации последствий компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации;
- требования к подразделениям и должностным лицам субъектов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Центры ГосСОПКА принято делить на три класса: А, Б, В, где класс А выполняет полный предусмотренный перечень, а класс В – только минимальное количество функций.

Одна из самых распространенных проблем при построении центров заключается в том, что организации на начальном этапе стремятся реализовать все заложенные функции, не имея при этом должного уровня базового функционала, что приводит к неудовлетворительным результатам выполнения возложенных на Центр задач, а это, в свою очередь, к финансовым потерям. Внедрение сложных технологий требует больших денежных и человеческих ресурсов.

Общий обзор источников [4–8] показывает, что Центры включают три ключевые подсистемы:

– процессы (стандартизированные и повторяемые процессы выявления и реагирования на инциденты);

– люди (специалисты, занимающиеся аналитикой, реагированием и обслуживанием технических средств);

– технологии (программное / программно-аппаратное обеспечение, которое выполняет сбор и обработку событий ИБ).

Таким образом, работа по созданию Центра заключается в планировании, организации и контроле над процессами, людьми и технологиями.

2. СТРУКТУРА ЦЕНТРА МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. ПРОЦЕССЫ ЦЕНТРА

Первой распространенной ошибкой организаций – создателей центров, как показывает опыт, является в первую очередь приобретение технологических решений, а во вторую – выстраивание ключевых процессов, подведение их под приобретенное ПО. Успешный опыт указывает на необходимость проработки и документирования всех процессов в рамках деятельности Центра.

Основные функции Центра сводятся к управлению инцидентами ИБ на определенных стадиях. Различные источники приводят несколько моделей жизненного цикла управления инцидентами [4, 6, 9], а наиболее подходящей концепцией следует считать NIST SP 800-61 Rev2 «Computer Security Incident Handling Guide» [10]. Она включает в себя 4 этапа: 1) подготовка, 2) обнаружение и анализ, 3) сдерживание, искоренение и восстановление и 4) постинцидентная деятельность. Рассмотрим их ниже [3].

Подготовка (1.1. Инвентаризация информационных ресурсов; 1.2. Проектирование схемы размещения средств мониторинга и их внедрение; 1.3. Сбор событий безопасности).

Этап подготовки предполагает с периодичностью в 3 месяца систематизировать сведения об информационной инфраструктуре заказчика, настройках значимых средств защиты; формировать перечень источников мониторинга для установки на них агентов сбора событий безопасности и т. д. (рисунок).

Обнаружение и анализ (2.1. Анализ событий безопасности и обнаружение компьютерных атак и инцидентов; 2.2. Прием сообщений о возможных компьютерных инцидентах от персонала и пользователей информационных ресурсов; 2.3. Регистрация компьютерных инцидентов).

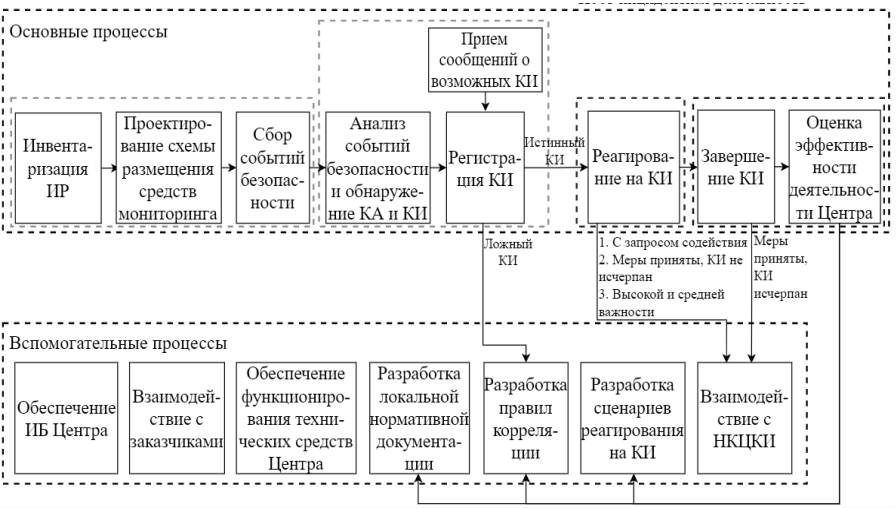
Анализ собранных на предыдущем этапе данных позволяет зафиксировать событие в форме компьютерного инцидента, выявить компьютерную атаку, а на основе правил корреляции автоматизировать процедуру сопоставления несвязных сведений, таким образом, выявив неочевидный компьютерный инцидент или атаку на основе индикаторов компрометации [7] с целью регистрации (рисунок).

Сдерживание, искоренение и восстановление (3.1. Реагирование на компьютерные инциденты и ликвидация их последствий).

Данный этап демонстрирует фактические действия в случае возникновения компьютерной атаки или инцидента в форме регламентов, сценариев

и инструкций с нацеленностью на формирование рекомендаций по обнаружению и ликвидации, а также предупреждению повторных инцидентов (рисунок).

Постинцидентная деятельность (4.1. Завершение компьютерного инцидента; 4.2. Оценка эффективности деятельности Центра) (рисунок).



Процессная модель Центра

Process model of the Center

На итоговом этапе происходит закрытие инцидента и оповещение НКЦКИ, организация хранения данных на установленный срок и оценивание эффективности работы Центра, а в случае несвоевременного обнаружения инцидента – совершенствование регламентов.

Также стоит отметить наличие вспомогательных процессов, которые осуществляются на различных этапах учета и управления инцидентами:

1) взаимодействие с НКЦКИ;

2) взаимодействие с заказчиками;

3) разработка локальной нормативной документации;

4) обеспечение функционирования технических средств Центра мониторинга информационных систем (далее – ИС);

5) обеспечение информационной безопасности Центра мониторинга ИБ;

6) разработка правил корреляции;

7) разработка сценариев реагирования на компьютерные инциденты.

Обобщение различных источников позволило предложить визуализацию модели деятельности Центра в формате процесса (см. рисунок).

2.2. СПЕЦИАЛИСТЫ ЦЕНТРА

Несмотря на то что человек считается слабым звеном в кибербезопасности, он является самым ценным ресурсом для Центра. Даже самые современные технологии не способны полностью исключить необходимость участия человека.

Как правило, выделяют три линии (уровня) специалистов Центра [4, 6, 11–13]:

- так называемая *первая линия* Центра занимается разбором поступающих событий информационной безопасности, выявлением и регистрацией инцидентов;
- так называемая *вторая линия* Центра занимается углубленным анализом инцидентов (если первая линия не в силах с этим справиться), реагированием на них, а также разработкой правил корреляции и сценариев реагирования;
- итоговая *третья линия* Центра обладает наиболее высокими компетенциями и проводит расследования инцидентов, занимается реверс-инжинирингом, тестированием на проникновение, threat hunting и threat intelligence и разработкой методик по выявлению инцидентов, противодействию компьютерным атакам и устранению их последствий.

Во главе многоуровневой структуры находятся управленческие роли, которые взаимодействуют со всеми линиями, а также с заказчиками.

Однако вышеописанная структура распределения специалистов существует только в теории, как «идеальный шаблон». В реальных же условиях модель может адаптироваться вплоть до совмещения всех функций в одном человеке. Чаще всего на практике границы между линиями размываются и аналитики первого уровня могут привлекаться к задачам второго уровня и так далее [14, 15].

2.3. ТЕХНОЛОГИИ ЦЕНТРА

Согласно [3] функции Центра выполняются с использованием следующих технических средств:

1) средство анализа событий безопасности;

2) средство учета и обработки инцидентов;

3) средство инвентаризации информационных ресурсов;

4) средство взаимодействия персонала.

В центре мониторинга ИБ могут не использоваться средства автоматизации реагирования, так как реагирование осуществляется силами заказчика.

Основным центральным средством анализа событий безопасности, а также учета и обработки компьютерного инцидента является SIEM-система (Security Information and Event Management). С помощью SIEM-систем должны быть реализованы следующие функции в соответствии с [3]:

1) сбор событий безопасности;

2) анализ событий безопасности и обнаружения компьютерных атак и инцидентов на основе правил корреляции;

3) регистрация компьютерных инцидентов вручную или автоматически;

4) формирование оповещения об обнаружении компьютерных инцидентов;

5) отправка карточки инцидента в НКЦКИ;

6) редактирование карточки инцидента.

Выбор SIEM-системы очень сильно зависит от рынка. Подходящие по функционалу решения, которые предлагает отечественный рынок и которые сертифицированы ФСТЭК России по 4-му уровню доверия:

1) Kaspersky Unified Monitoring and Analysis Platform (KUMA);

2) KOMRAD Enterprise SIEM;

3) MaxPatrol SIEM;

4) RuSIEM;

5) СёрчИнформ SIEM.

Для выбора Центра были установлены следующие критерии при выборе SIEM-системы:

- высокая производительность при небольших требованиях к аппаратной части;
- гибкое подключение источников событий безопасности;
- возможность поиска по событиям;
- возможность разработки пользовательских правил корреляции;
- возможность интеграции с Центром ГосСОПКА;
- возможность масштабирования;
- простота развертывания и эксплуатации. Сравнение вышеприведенных SIEM-систем представлено в таблице.

Сравнение SIEM-систем

Comparison of SIEM systems

	KUMA	KOMRAD Enterprise SIEM	MaxPatrol SIEM	RuSIEM	СёрчИнформ SIEM
Минимальные требования к аппаратной части	CPU: 8 ядер RAM: 32 ГБ HDD: 500 ГБ	CPU: 2 ядра RAM: 2 ГБ HDD: 100 ГБ	CPU: 56 ядер RAM: 128 ГБ HDD: 2,4 ТБ	CPU: 4-8 ядер RAM: 16 ГБ HDD: 400 ГБ	CPU: 4 ядер RAM: 4 ГБ HDD: 200 ГБ
Возможность гибкого подключения источников	Да	Да	Да	Да	Да
Возможность поиска по событиям	Да	Да	Да	Да	Нет
Разработка собственных правил корреляции	Да	Да	Да	Да	Да
Интеграция с ГосСОПКА	Да	Да	Да	Да	Да
Возможность масштабирования	Да	Да	Да	Да	Да
Простота использования	Да	Да	Нет	Нет	Да

ЗАКЛЮЧЕНИЕ

Таким образом, сбор, анализ литературных и иных источников позволил сформировать последовательность действий, позволяющих, учитывая требования действующего законодательства и зарубежного опыта, создать рабочий вариант Центра. В статье приведены рекомендации по основным структурным компонентам Центра, приведено сравнение ключевой технологии – SIEM – системы, что может позволить принимать решение по ее выбору.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kii/285-zakony/1610-federalnyj-zakon-ot-26-%20iyulya-2017-g-n-187-fz (дата обращения: 08.12.2022).

2. Указ Президента Российской Федерации от 15.01.2013 г. № 31 «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Россий-

ской Федерации». – URL: https://base.garant.ru/70299068/ (дата обращения: 08.12.2022).

3. Методические рекомендации ФСБ России от 24.12.2016 № 149/2/7-200 «Методические рекомендации по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

4. Grasp on next generation security operation centre (NGSOC): Comparative study / Y.T. Dun, M.F.A. Razak, M.F. Zolkipli, T.F. Bee, A. Firdaus // International Journal of Nonlinear Analysis and Applications. – 2021. – Vol. 12 (2). – P. 869–895. – URL: https://ijnaa.semnan.ac.ir/article_5145.html (accessed: 08.12.2022).

5. *Chamkar S.A., Maleh Y., Gherabi N.* The human factor capabilities in Security Operation Center (SOC) // Lecture Notes in Networks and Systems. – 2021. – Vol. 357. – P. 579–590. – DOI: 10.1080/07366981.2021.1977026.

6. Security Operations Center: A systematic study and open challenges / M. Vielberth, F. Böhm, I. Fichtinger, G. Pernul // IEEE Access. – 2020. – Vol. 8. – P. 227756–227779. – DOI: 10.1109/ACCESS.2020.3045514.

7. Создание собственного SOC при помощи классификации MITRE и openssource стека elk / Я.В. Степанов, Т.Н. Копышева, Т.В. Митрофанова, Т.Н. Смирнова // Информационные технологии в науке, управлении и образовании: междисциплинарный подход и тенденции развития: сборник материалов Всероссийской научно-практической конференции. – Димитровград, 2021. – С. 229–236. – URL: https://elibrary.ru/item.asp?id=47424688 (дата обращения: 08.12.2022).

8. *Knerler K., Parker I., Zimmerman C.* 11 strategies of a world-class cybersecurity operations center. – MITRE, 2022. – URL: https://www.mitre.org/news-insights/publication/11-strategies-world-class-cybersecurity-operations-center (accessed: 08.12.2022).

9. *Mutemwa M., Mtsweni J., Zimba L.* Integrating a Security Operations Centre with an organization's existing procedures, policies and information technology systems // 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC). – IEEE, 2018. – P. 1–6. – DOI: 10.1109/ICONIC.2018.8601251.

10. NIST SP 800-61 Rev. 2. Computer Security Incident Handling Guide / National Institute of Standards and Technology. – NIST, 2012. – URL: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final (accessed: 08.12.2022).

11. *János F.D., Huu Phuoc Dai N.* Security concerns towards Security Operations Centers // 2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI). – IEEE, 2018. – P. 000273–000278. – DOI: 10.1109/SACI.2018.8440963.

12. Towards a framework for measuring the performance of a Security Operations Center analyst / E. Agyepong, Y. Cherdantseva, P. Reinecke, P. Burnap // International Conference on Cyber Security and Protection of Digital Services (Cyber Security). – IEEE, 2020. – P. 1–8. – DOI: 10.1109/CyberSecurity49315.2020.9138872.

13. *Hámornik B.P., Krasznay C., Nicholson D.* A team-level perspective of human factors in cyber security: Security Operations Centers // Advances in Human Factors in Cybersecurity. – Cham: Springer, 2018. – P. 234–236. – DOI: 10.1007/978-3-319-60585-2_21.

14. *Шабловский Я.К., Гельфанд А.М.* Обзор технологии SOC (Security Operations Center) // Инновации. Наука. Образование. – 2021. – № 33. – С. 1316–1321. – URL: https://www.elibrary.ru/item.asp?id=46168786 (дата обращения: 08.12.2022).

15. *Abd Majid M., Zainol Ariffin K.A.* Model for successful development and implementation of Cyber Security Operations Centre (SOC) // PLoS One – 2021. – Vol. 16 (11). – DOI: 10.1371/journal.pone.0260157.

Киселев Антон Анатольевич, старший преподаватель кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – методы выявления внутреннего нарушителя. E-mail: anton.kiselev@corp.nstu.ru

Коротких Игорь Валерьевич, начальник Центра мониторинга информационных систем ООО «СИБ». Область научных интересов – методы исследования сетевого трафика. E-mail: kiv@sib-nsk.net

Шотт Валерия Владиславовна, аналитик компании «Инфосистемы Джет». Область научных интересов – методы анализа трафика. E-mail: shottvv@mail.ru

DOI: 10.17212/2782-2230-2022-4-39-51

The practice of making a Security Operations Center*

A.A. Kiselev[1], I.V. Korotkikh[2], V.V. Shott[3]

[1] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, senior lecturer of the Information Security Department. E-mail: anton.kiselev@corp.nstu.ru*
[2] *LLC "Information Security Systems", 63/1 Borisa Bogatkova Street, Novosibirsk, 630008, Russian Federation, head of the Information Systems Monitoring Center. E-mail: kiv@sibnsk.net*
[3] *Jet Infosystems, 14/1 Bolshaya Novodmitrovskaya Street, Moscow, 127015, Russian Federation, analysts. E-mail: shottvv@mail.ru*

The rapidly changing landscape of information security threats, directly related to the development of information technologies, requires continuous automated monitoring of information security events for the purpose of quick response, retrospective analysis for targeted attacks, as well as compliance with the requirements of the regulators of the sphere. This article presents the process of creating a concept that is being implemented everywhere – an information security monitoring center. This complex, multifactorial process takes into account the elaboration of regulatory legal acts and regulatory and methodological documentation, the analysis of current international practices, the formation of a pool of technologies used, the formation of a service team and the debugging of workflows. At the same time, the possibility of the SOC's interaction with regulatory authorities, the specific of communication with customers, its own resistance to attacks, economic feasibility, the peculiarities of human psychology, etc. should be taken into account. To visualize the work of the SOC, a process diagram of the SOC's work is presented. In the article attention is paid to the choice of the core of the SOC – SIEM system. The result clearly represents the current cross-section of the Russian market of systems of this class, which is important in the context of import substitution.

Keywords: SOC, information security monitoring center, information security monitoring, computer incident, computer attack, GosSOPKA, SIEM

REFERENCES

1. Federal Law of July 26, 2017 N 187 "On the Security of Critical Information Infrastructure of the Russian Federation". (In Russian). Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kii/285-zakony/1610-federalnyj-zakon-ot-26-%20iyulya-2017-g-n-187-fz (accessed 08.12.2022).

2. Decree of the President of the Russian Federation of January 15, 2013 N 31s "On the creation of a state system for detecting, preventing and eliminating the con-

* *Received 21 October 2022.*

sequences of computer attacks on information resources of the Russian Federation". (In Russian). Available at: https://base.garant.ru/70299068/ (accessed 08.12.2022).

3. Recommendations of the Federal Security Service of Russia dated December 24, 2016 N 149/2/7-200 "Methodological recommendations for the creation of departmental and corporate centers of the state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation". (In Russian).

4. Dun Y.T., Razak M.F.A., Zolkipli M.F., Bee T.F., Firdaus A. Grasp on next generation security operation centre (NGSOC): Comparative study. *International Journal of Nonlinear Analysis and Applications*, 2021, vol. 12 (2), pp. 869–895. Available at: https://ijnaa.semnan.ac.ir/article_5145.html (accessed 08.12.2022).

5. Chamkar S.A., Maleh Y., Gherabi N. The human factor capabilities in Security Operation Center (SOC). *Lecture Notes in Networks and Systems*, 2021, vol. 357, pp. 579–590. DOI: 10.1080/07366981.2021.1977026.

6. Vielberth M., Böhm F., Fichtinger I., Pernul G. Security Operations Center: A systematic study and open challenges. *IEEE Access*, 2020, vol. 8, pp. 227756–227779. DOI: 10.1109/ACCESS.2020.3045514.

7. Stepanov Ya.V., Kopysheva T.N., Mitrofanova T.V., Smirnova T.N. [Creating your own SOC using the MITRE classification and the openssource elk stack]. *Informatsionnye tekhnologii v nauke, upravlenii i obrazovanii: mezhdistsiplinarnyi podkhod i tendentsii razvitiya* [Information Technologies in Science, Management and Education: Interdisciplinary approach and Development trends]. Collection of materials of the All-Russian Scientific and Practical Conference, Dimitrovgrad, 2021, pp. 229–236. (In Russian). Available at: https://elibrary.ru/item.asp?id=47424688 (accessed 08.12.2022).

8. Knerler K., Parker I., Zimmerman C. *11 strategies of a world-class cybersecurity operations center*. MITRE, 2022. Available at: https://www.mitre.org/news-insights/publication/11-strategies-world-class-cybersecurity-operations-center (accessed 08.12.2022).

9. Mutemwa M., Mtsweni J., Zimba L. Integrating a Security Operations Centre with an organization's existing procedures, policies and information technology systems. *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*. IEEE, 2018, pp. 1–6. DOI: 10.1109/ICONIC.2018.8601251.

10. NIST SP 800-61 Rev. 2. *Computer Security Incident Handling Guide*. National Institute of Standards and Technology, 2012. Available at: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final (accessed 08.12.2022).

11. János F.D., Huu Phuoc Dai N. Security concerns towards Security Operations Centers. *2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI)*. IEEE, 2018, pp. 000273–000278. DOI: 10.1109/SACI.2018.8440963.

12. Agyepong E., Cherdantseva Y., Reinecke P., Burnap P. Towards a framework for measuring the performance of a Security Operations Center analyst. *International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. IEEE, 2020, pp. 1–8. DOI: 10.1109/CyberSecurity49315.2020.9138872.

13. Hámornik B.P., Krasznay C., Nicholson D. A team-level perspective of human factors in cyber security: Security Operations Centers. *Advances in Human Factors in Cybersecurity*. Cham, Springer, 2018, pp. 234–236. DOI: 10.1007/978-3-319-60585-2_21.

14. Shablovskii Ya.K., Gel'fand A.M. Obzor tekhnologii SOC (Security Operations Center) [Review of SOC technology (Security Operations Center)]. *Innovatsii. Nauka. Obrazovanie*, 2021, no. 33, pp. 1316–1321. (In Russian). Available at: https://www.elibrary.ru/item.asp?id=46168786 (accessed 08.12.2022).

15. Abd Majid M., Zainol Ariffin K.A. Model for successful development and implementation of Cyber Security Operations Centre (SOC). *PLoS One*, 2021, vol. 16 (11). DOI: 10.1371/journal.pone.0260157.

Для цитирования:

Киселев А.А., Коротких И.В., Шотт В.В. Практика создания Центра мониторинга информационной безопасности // Безопасность цифровых технологий. – 2022. – № 4 (107). – С. 39–51. – DOI: 10.17212/2782-2230-2022-4-39-51.

For citation:

Kiselev A.A., Korotkikh I.V., Shott V.V. Praktika sozdaniya tsentra monitoringa informatsionnoi bezopasnosti [The practice of making a Security Operations Center]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2022, no. 4 (107), pp. 39–51. DOI: 10.17212/2782-2230-2022-4-39-51.