**БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 4 (111).** – 9–23

## *АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ И ПРОИЗВОДСТВАМИ*

УДК 004.056 DOI: 10.17212/2782-2230-2023-4-9-23

# МЕТОДИКА ОРГАНИЗАЦИИ ПРОЦЕССА МОНИТОРИНГА РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ*

А.В. ИВАНОВ[1], И.А. ОГНЕВ[2], И.В. НИКРОШКИН[3], Ю.А. ПОПОВА[4]

[1] *630090, РФ, г. Новосибирск, пр. Академика Лаврентьева, 6, Институт вычислительной математики и математической геофизики Сибирского отделения Российской академии наук, старший научный сотрудник лаборатории искусственного интеллекта и информационных технологий. E-mail: andrej.ivanov@corp.nstu.ru*

[2] *630090, РФ, г. Новосибирск, пр. Академика Лаврентьева, 6, Институт вычислительной математики и математической геофизики Сибирского отделения Российской академии наук, инженер лаборатории искусственного интеллекта и информационных технологий. E-mail: i.ognev.2016@corp.nstu.ru*

[3] *630090, РФ, г. Новосибирск, пр. Академика Лаврентьева, 6, Институт вычислительной математики и математической геофизики Сибирского отделения Российской академии наук, инженер лаборатории искусственного интеллекта и информационных технологий. E-mail: i.nikroshkin@corp.nstu.ru*

[4] *630073, РФ, г. Новосибирск, пр. К. Маркса, 20, Новосибирский государственный технический университет, лаборант инжинирингового центра «Информационная безопасность». E-mail: yu.popova.2019@stud.nstu.ru*

Статья посвящена методике организации процесса мониторинга распределенных информационных систем. Рассмотрена общая концепция построения процесса мониторинга информационной безопасности. Особое внимание уделено таким недостаткам распределенных систем, как проблемы администрирования системы, проблемы ограниченности масштабируемости распределенных систем и проблемы переносимости программного обеспечения. Был сделан вывод о том, что в настоящее время нет единого подхода для устранения указанных недостатков при построении процесса мониторинга. Приведена модель децентрализованной распределенной системы, для которой разработана методика организации процесса мониторинга. Описано три подхода к организации процесса мониторинга распределенных информационных систем, а именно: организация мониторинга сетевой активности информационной системы, организация мониторинга хостовой активности информационной системы и смешанный подход. В методике используется смешанный подход, основанный на мониторинге сетевой и хостовой активности. Рассмотрен процесс приоритизации источников событий информационной безопасности, который включает в себя оценку рисков

* Статья получена 10 ноября 2023 г.

ИБ, выявление актуальных угроз ИБ и критичных активов организации. В результате предложена методика организации процесса мониторинга распределенных информационных систем, состоящая из четырех этапов: расчета рисков, определения актуальных угроз, приоритизации источников событий информационной безопасности и подключения выбранных источников к системе мониторинга событий информационной безопасности.

**Ключевые слова**: информационная безопасность, кибербезопасность, мониторинг, распределенные информационные системы, центр мониторинга, SOC, события информационной безопасности, инциденты информационной безопасности

## ВВЕДЕНИЕ

Многие организации принимают во внимание современные угрозы информационной безопасности из-за постоянных компьютерных атак. Злоумышленники могут находиться в сети компании до 15 дней [1], прежде чем их обнаружат, что приводит к финансовым потерям. В 2018 году крупные компании пострадали от атаки вируса-шифровальщика. В прошлом году случаи утечки конфиденциальной информации и шпионажа увеличились, и этот год не исключение. Поиск решений для минимизации таких рисков сейчас очень актуален.

Построение Security Operation Center (SOC), который объединяет программное обеспечение, аппаратное обеспечение, персонал и процессы, является эффективным решением для обеспечения информационной безопасности [2, 3]. SOC предназначен для централизованного сбора и анализа информации об инцидентах информационной безопасности, поступающей из различных источников ИТ-инфраструктуры. Этот подход является ключевым компонентом в обеспечении информационной безопасности организации, поскольку он направлен на мониторинг, обнаружение и оперативную реакцию на инциденты, что в результате способствует снижению возможных негативных последствий.

Работа выполнена в рамках государственного задания ИВМиМГ СО РАН № 0251-2022-0005.

## 1. ФОРМИРОВАНИЕ ПРОБЛЕМАТИКИ

Построение SOC в сфере информационной безопасности является одной из наиболее популярных тем на сегодняшний день [4]. Существует множество работ, содержащих руководство по выстраиванию процессов мониторинга информационной безопасности, интеграции программных решений и выбору источников событий для выявления компьютерных атак и инцидентов ин-

формационной безопасности [5–7]. Общая концепция структурно выглядит следующим образом:

1) планирование;
2) проектирование;
3) строительство;
4) управление;
5) рефлексия.

Информационные системы можно разделить по географическому признаку на распределенные и нераспределенные. В нераспределенных информационных системах и централизованных распределенных системах процесс выстраивания мониторинга достаточно проработан в силу относительной простоты, так как в нераспределенной системе вся информация находится в ведении одной внутренней структуры, а в централизованной распределенной системе все ее сегменты построены по одинаковому принципу. Более сложная задача – выстроить эффективный процесс мониторинга в децентрализованной распределенной системе, разными частями которой заведуют разные подразделения в условиях отсутствия общих требований в построении и администрировании сетей.

Распределенные системы имеют свои особенности:

- проблемы администрирования, включая балансирование нагрузки и восстановление данных при ошибках;
- ограничения масштабируемости;
- проблемы переносимости программного обеспечения.

Основные проблемы администрирования в распределенных системах:

- балансировка нагрузки на узлы системы;
- восстановление данных при ошибке;
- сбор статистики с узлов системы;
- автоматическое обновление программного обеспечения на узлах системы.

Ограничения масштабируемости – это действительно одна из ключевых проблем при проектировании распределенных систем. Распределенные системы помогли избежать ограничений возможности увеличения вычислительной мощности. Существует три основных показателя масштабируемости системы [8]:

- масштабируемость относительно размера, что позволяет простое подключение новых узлов;
- географическая масштабируемость, позволяющая подключать новые узлы к сети без привязки к конкретной географической зоне;

• масштабируемость управления, означающая, что администрирование системы не становится более сложным при увеличении общего количества узлов.

Проблема переносимости программного обеспечения действительно ограничивает развитие и расширение распределенных систем. Быстрое развитие программных архитектур, языков программирования и ИТ-индустрии в целом требует разработки методологий для обеспечения переносимости программного кода.

В области мониторинга информационной безопасности актуальными проблемами распределенных систем являются проблемы администрирования, переносимости ПО, а также прозрачности системы [9]. Под прозрачностью системы будем понимать восприятие системы как однородного объекта, а не набора автономных сервисов. Решение данных проблем связано с уровнями стратегии построения SOC.

Если проблемы на 3-м и 4-м этапе решены силами вендоров систем мониторинга событий информационной безопасности [10–12], то для решения проблем на 1-м и 2-м этапе нет единого подхода.

## 2. ОСНОВНЫЕ ЭЛЕМЕНТЫ МЕТОДИКИ

### 2.1. РАСПРЕДЕЛЕННЫЕ СИСТЕМЫ

Распределенные системы можно представить как неполносвязный граф [13] (рис. 1).

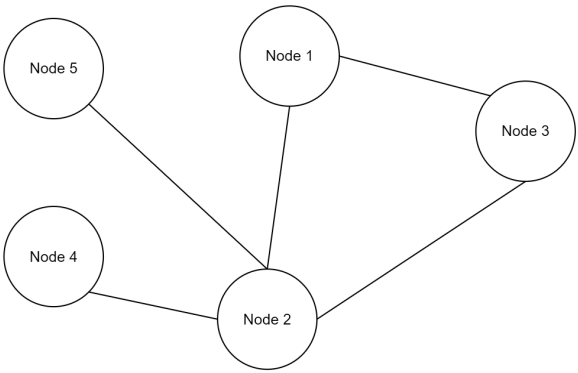


*Рис. 1.* Модель распределенной системы

*Fig. 1.* Distributed System Model

Однако в то время как в [13] распределенная система рассматривается как совокупность вычислительных узлов, в нашем случае необходимо рассматривать распределенную систему как совокупность самостоятельных систем (рис. 2).

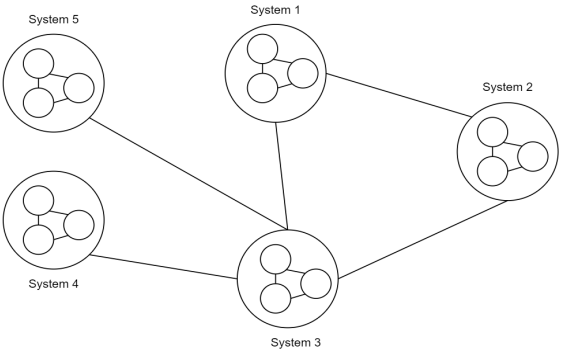


*Рис. 2.* Распределенная система как совокупность систем

*Fig. 2.* Distributed system as a set of systems

При рассмотрении такой модели будем считать, что каждая отдельная система строится по заранее заданному шаблону организацией, при этом состав систем и связи внутри системы похожи друг на друга. Обратим внимание на более сложный случай – децентрализованную распределенную систему (рис. 3). Децентрализованная распределенная система – распределенная система, в которой каждый узел-система имеет уникальный состав и внутренние связи.

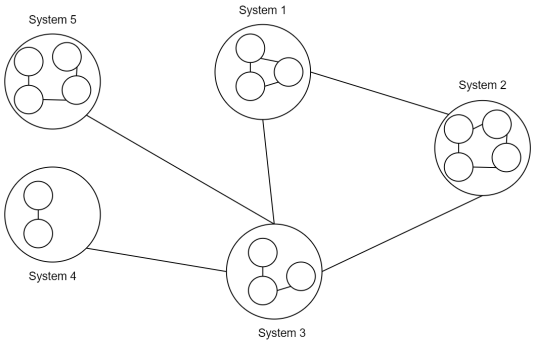


*Рис. 3.* Децентрализованная распределенная система

*Fig. 3.* Decentralized Distributed System

Далее под распределенной системой будем подразумевать децентрализованную распределенную систему (рис. 3) как самый сложный случай для построения процесса мониторинга событий информационной безопасности.

## 2.2. ПОДХОДЫ К ОРГАНИЗАЦИИ ПРОЦЕССА МОНИТОРИНГА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

К вопросу организации процесса мониторинга информационных систем можно подойти с помощью трех подходов:

1) организации мониторинга сетевой активности информационной системы [14, 15];

2) организации мониторинга хостовой активности информационной системы [16, 17];

3) смешанного подхода, основанного на мониторинге сетевой и хостовой активности [18, 19].

Рассматривая первый случай, можно выделить достоинство в том, что зачастую мониторинг организуется сбором событий информационной безопасности с физической или логической границы сети – это позволяет упростить интеграцию системы мониторинга событий информационной безопасности в любые распределенные и нераспределенные системы. Однако данный подход имеет довольно большой недостаток: при мониторинге создается неполная картина активности информационной системы.

Второй случай также не лишен недостатка – ограниченности видимости активности внутри информационной системы. Однако помимо этого недостатка имеется еще один – сложность интеграции в децентрализованные распределенные информационные системы, так как не удается создать единый подход к выбору и подключению источников событий информационной безопасности.

Третий случай, с одной стороны, объединяет все недостатки предыдущих двух подходов, однако имеет одно главное преимущество: одновременный анализ сетевой и хостовой активности позволяет создать полную видимость активности внутри информационной системы и прозрачность каждого узла-системы для службы информационной безопасности и, как следствие, для ИТ-служб.

В нашей работе будет использоваться смешанный подход к построению процесса мониторинга событий информационной безопасности децентрализованных распределенных информационных систем, однако предстоит найти решение для преодоления недостатка, касающегося большой сложности вы-

бора источников событий информационной безопасности в силу уникальности каждого узла-системы. Эта проблема решается использованием инвентаризации и последующей приоритизацией потенциальных источников событий информационной безопасности.

### 2.3. ПРИОРИТИЗАЦИЯ ИСТОЧНИКОВ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Приоритизация источников событий информационной безопасности является одним из следствий, которое можно извлечь из процесса управления рисками. Управление рисками – процесс, заключающийся в выявлении, идентификации и оценке рисков ИБ, которые могут привести к недопустимым событиям и (или) невыполнению бизнес-целей организации [20].

Результат процесса управления рисками – список рисков ИБ, актуальных для организации. Этот список рисков можно переложить в плоскость актуальных угроз ИБ [21]. Модель угроз содержит в себе модели нарушителя, а также возможные векторы компьютерной атаки на информационную систему [21, 22].

Таким образом, приоритизация источников событий информационной безопасности выглядит следующим образом:

1) оценка рисков ИБ;

2) выявление актуальных угроз ИБ;

3) выявление критичных активов, которые могут быть подвержены компьютерным атакам или могут содержать в себе следы компрометации компьютерного инцидента.

## 3. МЕТОДИКА ОРГАНИЗАЦИИ ПРОЦЕССА МОНИТОРИНГА РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Для организации эффективного процесса мониторинга распределенных информационных систем необходимо подключить к системе мониторинга критичные активы и активы, которые могут свидетельствовать о компрометации любого сегмента информационной системы. Для процесса мониторинга используется модель подключения сетевых и хостовых источников событий информационной безопасности.

1. Расчет рисков.

Для расчета рисков ИБ необходимо определить следующие сущности:

– основные и вспомогательные бизнес-процессы организации;

– распределение бизнес-процессов по распределенным сегментам информационной системы;

– выявление недопустимых событий организации;

– определение защищаемых активов в соответствии с требованиями федеральных органов исполнительной власти, ответственных за обеспечение безопасности государственных информационных систем, информационных систем персональных данных, автоматизированных систем управления производственными и технологическими процессами, критической информационной инфраструктуры Российской Федерации.

Далее необходимо оценить критичность выявленных бизнес-процессов – выполнить оценку экономических, репутационных потерь при нарушении нормальной деятельности бизнес-процесса.

2. Определение актуальных угроз.

Необходимо выявить актуальные угрозы ИБ, которые могут привести к реализации недопустимых событий, выявить актуальных нарушителей и возможные векторы реализации компьютерных атак. Такую деятельность необходимо провести в каждом сегменте распределенной информационной системы.

3. Приоритизация источников событий информационной безопасности.

Исходя из векторов возможных компьютерных атак выявить критические системы, непрерывность деятельности которых может привести к недопустимым событиям для организации. Чем выше возможный ущерб для организации, тем выше приоритет у целевого актива.

Для каждого сегмента распределенной системы необходимо составить свой список.

4. Подключение выбранных источников к системе мониторинга событий информационной безопасности.

Используя функционал современных систем мониторинга событий информационной безопасности, необходимо разместить в каждом сегменте сети сборщика (коллектор, агент) событий информационной безопасности. Для обеспечения связи с единым центром обработки событий информационной безопасности каждый сборщик должен передавать события информационной безопасности по защищенному каналу передачи информации.

Каждый сегмент распределенной системы должен обеспечить непрерывную или близкую к непрерывной передачу событий информационной безопасности.

Итого, каждый сегмент распределенной информационной системы должен быть полностью изучен, и должны быть выявлены критические активы, за которыми необходим постоянный мониторинг их безопасности. Подключение всех критичных активов в централизованный центр обработки событий информационной безопасности позволит обеспечить прозрачность каждого

сегмента информационной системы и обеспечить централизацию управления событиями информационной безопасности.

## ЗАКЛЮЧЕНИЕ

В настоящее время отсутствует единый подход для решения проблем, которые возникают при построении процесса мониторинга информационной безопасности распределенных систем. В связи с этим была разработана методика, которая позволяет решить проблемы администрирования системы и переносимости программного обеспечения. Разработанная методика включает в себя четыре этапа.

1. Расчет рисков – классификация основных и вспомогательных бизнес-процессов по распределенным сегментам ИС и выявление недопустимых событий для определения критичных ИТ-активов.

2. Определение актуальных угроз – выявление актуальных угроз ИБ, нарушителей и векторов реализации атак в каждом сегменте ИС.

3. Приоритизация источников событий информационной безопасности – составление списка критичных активов, для которых необходим постоянный мониторинг безопасности.

4. Подключение выбранных источников к системе мониторинга событий информационной безопасности – обеспечение непрерывной передачи событий ИБ в каждом сегменте распределенной ИС.

## СПИСОК ЛИТЕРАТУРЫ

1. По данным Sophos, время пребывания злоумышленников в сети увеличилось на 36 % // SecurityLab.ru. – 2022, 9 июня. – URL: https://www.securitylab.ru/finance_news/532207 (дата обращения: 01.12.2023).

2. *Стрельников Р.В.* SOC. Неэффективность внедрения // Вестник Балтийского федерального университета им. И. Канта. Серия: Физико-математические и технические науки. – 2019. – № 4. – С. 81–85.

3. *Muniz J., McIntyre G., AlFardan N.* Security operations center: building, operating, and maintaining your SOC. – Cisco Press, 2015. – URL: http://www.ciscopress.com/store/security-operations-center-building-operating-and-maintaining-9780134052076 (accessed: 01.12.2023).

4. Создание и управление Security Operations Center для эффективного применения в реальных условиях / А.А. Казанцев, А.В. Красов, А.И. Катасонов, А.М. Гельфанд // Актуальные проблемы инфотелекоммуникаций

в науке и образовании: VIII Международная научно-техническая и научно-методическая конференция. – СПб.: СПбГУТ, 2019. – С. 590–595.

5. *Mughal A.A.* Building and securing the modern Security Operations Center (SOC) // International Journal of Business Intelligence and Big Data Analytics. – 2022. – Vol. 5 (1). – P. 1–15.

6. *Alahmadi B.A., Axon L., Martinovic I.* 99 % false positives: a qualitative study of SOC analysts' perspectives on security alarms // 31st USENIX Security Symposium. – Boston: USENIX Association, 2022. – P. 2783–2800.

7. *Shahjee D., Ware N.* Integrated network and Security Operation Center: a systematic analysis // IEEE Access. – 2022. – Vol. 10. – P. 27881–27898.

8. *Таненбаум Э., Стеен М. ван.* Распределенные системы. Принципы и парадигмы. – СПб.: Питер, 2003. – 876 с.

9. *Цветков В.Я., Алпатов А.Н.* Проблемы распределенных систем // Перспективы науки и образования. – 2014. – № 6 (12). – С. 31–36.

10. Об установке конвейеров обработки событий // Positive Technologies. Документация по продуктам. – URL: https://help.ptsecurity.com/projects/siem/latest/ru-RU/help/3690716683 (дата обращения: 01.11.2023).

11. KOMRAD Enterprise SIEM // Эшелон. Комплексная безопасность. – URL: https://npo-echelon.ru/production/65/11793 (дата обращения: 01.11.2023).

12. RuSIEM. – URL: https://rusiem.com/ru/products/rusiem (дата обращения: 01.11.2023).

13. *Дурнов Р.В.* Модель распределенной вычислительной сети // Известия ТулГУ. Технические науки. – 2022. – № 9. – С. 151–153.

14. *Дудникова А.И.* Разработка системы мониторинга сетевого трафика на базе Flow-протоколов // Молодежь. Общество. Современная наука, техника и инновации. – 2021. – № 20. – С. 193–195. – Яз. англ.

15. *Kim S., Park K.-J., Lu C.* A survey on network security for cyber–physical systems: from threats to resilient design // IEEE Communications Surveys & Tutorials. – 2022. – Vol. 24 (3). – P. 1534–1573. – DOI: 10.1109/COMST.2022.3187531.

16. Host-based IDS: a review and open issues of an anomaly detection system in IoT / I. Martins, J.S. Resende, P.R. Sousa, S. Silva, L. Antunes, J. Gama // Future Generation Computer Systems. – 2022. – Vol. 133. – P. 95–113.

17. *Formby D., Beyah R.* Temporal execution behavior for host anomaly detection in programmable logic controllers // IEEE Transactions in Information Forensics and Security. – 2020. – Vol. 15. –P. 1455–1469.

18. *Skendžić A., Kovačić B., Balon B.* Management and monitoring security events in a business organization – SIEM system // 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO). – Opatija: IEEE, 2022. – P. 1203–1208.

19. *Thursday Ehis A.-m.* Optimization of security information and event management (SIEM) infrastructures, and events correlation/regression analysis for optimal cyber security posture // Archives of Advanced Engineering Science. – 2023. – P. 1–10. – DOI: 10.47852/bonviewAAES32021068.

20. *Бирюков С.А., Дьяков С.А.* Применение методики управления рисками в малых и средних строительных организациях // Вестник Академии знаний. – 2021. – № 42 (1). – С. 36–45.

21. Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix / W. Xiong, E. Legrand, O. Åberg, R. Lagerström // Software and Systems Modeling. – 2022. – Vol. 21 (1). – P. 157–177. – DOI: 10.1007/s10270-021-00898-7.

22. Методический документ «Методика оценки угроз безопасности информации» от 5 февраля 2021 г. (с изм. и доп. в ред. от 06.12.2022). – ФСТЭК России, 2021.

***Иванов Андрей Валерьевич***, старший научный сотрудник лаборатории искусственного интеллекта и информационных технологий Института вычислительной математики и математической геофизики Сибирского отделения Российской академии наук. E-mail: andrej.ivanov@corp.nstu.ru

***Огнев Игорь Александрович***, инженер лаборатории искусственного интеллекта и информационных технологий Института вычислительной математики и математической геофизики Сибирского отделения Российской академии наук. E-mail: i.ognev.2016@corp.nstu.ru

***Никрошкин Иван Владимирович***, инженер лаборатории искусственного интеллекта и информационных технологий Института вычислительной математики и математической геофизики Сибирского отделения Российской академии наук. E-mail: i.nikroshkin@corp.nstu.ru

***Попова Юлия Александровна***, лаборант инжинирингового центра «Информационная безопасность» Новосибирского государственного технического университета. E-mail: yu.popova.2019@stud.nstu.ru

DOI: 10.17212/2782-2230-2023-4-9-23

# Methodology for organizing the process of monitoring of distributed information systems*

**A.V. Ivanov[1], I.A. Ognev[2], I.V. Nikroshkin[2], J.A. Popova[4]**

[1] *Institute of Computational Mathematics and Mathematical Geophysics of Siberian Branch of Russian Academy of Sciences, 6 Akademika Lavrentiev Avenue, Novosibirsk, 630090, Russian Federation, senior researcher at the laboratory of Artificial Intelligence and Information Technologies. E-mail: andrej.ivanov@corp.nstu.ru*

[2] *Institute of Computational Mathematics and Mathematical Geophysics of Siberian Branch of Russian Academy of Sciences, 6 Akademika Lavrentiev Avenue, Novosibirsk, 630090, Russian Federation, engineer at the laboratory of Artificial Intelligence and Information Technologies. E-mail: i.ognev.2016@corp.nstu.ru*

[3] *Institute of Computational Mathematics and Mathematical Geophysics of Siberian Branch of Russian Academy of Sciences, 6 Akademika Lavrentiev Avenue, Novosibirsk, 630090, Russian Federation, engineer at the laboratory of Artificial Intelligence and Information Technologies. E-mail: i.nikroshkin@corp.nstu.ru*

[4] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, laboratory assistant at the engineering center "Information Security". E-mail: yu.popova.2019@stud.nstu.ru*

This article is devoted to the methodology of organizing the process of monitoring of distributed information systems. The article considers the general concept of building the process of information security monitoring. Special attention is paid to such disadvantages of distributed systems as problems of system administration, problems of limited scalability of distributed systems and problems of software portability. It was concluded that at present there is no unified approach to eliminate these disadvantages when building a monitoring process. The model of decentralized distributed system for which the methodology of monitoring process organization is developed is given. Three approaches to the organization of monitoring process of distributed information systems are described, namely the organization of monitoring of network activity of information system, the organization of monitoring of host activity of information system and mixed approach. The mixed approach based on monitoring of network and host activity is used in the methodology. The process of prioritization of sources of information security events is considered, which includes the assessment of IS risks, identification of actual IS threats and identification of critical assets of the organization. As a result, a methodology for organizing the process of monitoring distributed information systems is proposed, which consists of four stages: risk calculation, identification of actual threats, prioritization of information security event sources and connection of selected sources to the information security event monitoring system.

**Keywords**: information security, cybersecurity, monitoring, distributed information systems, monitoring center, SOC, information security events, information security incidents

* *Received 10 November 2023.*

**REFERENCE**

1. Po dannym Sophos, vremya prebyvaniya zloumyshlennikov v seti uvelichilos' na 36 % [According to Sophos, the time attackers spend on the network has increased by 36 %]. *SecurityLab.ru*, 2022, 9 June. (In Russian). Available at: https://www.securitylab.ru/finance_news/532207 (accessed 01.11.2023).

2. Strelnikov R.V. SOC. Neeffektivnost' vnedreniya [SOC. Inefficiency of implementation]. *Vestnik Baltiiskogo federal'nogo universiteta im. I. Kanta. Seriya: Fiziko-matematicheskie i tekhnicheskie nauki = Vestnik of Immanuel Kant Baltic Federal University. Series: Physical-mathematical and technical sciences*, 2019, no. 4, pp. 81–85.

3. Muniz J., McIntyre G., AlFardan N. *Security operations center: building, operating, and maintaining your SOC*. Cisco Press, 2015. Available at: http://www.ciscopress.com/store/security-operations-center-building-operating-and-maintaining-9780134052076 (accessed 01.12.2023).

4. Kazantsev A., Krasov A., Katasonov A., Gelfand A. [Formation and control of Security Operations Center (SOC) for efficient using in practice]. *Aktual'nye problemy infotelekommunikatsii v nauke i obrazovanii*. VIII Mezhdunarodnaya nauchno-tekhnicheskaya i nauchno-metodicheskaya konferentsiya [8th International Conference on Advanced Infotelecommunications ICAIT 2019]. St. Petersburg, 2019, pp. 590–595. (In Russian).

5. Mughal A.A. Building and securing the modern Security Operations Center (SOC). *International Journal of Business Intelligence and Big Data Analytics*, 2022, vol. 5 (1), pp. 1–15.

6. Alahmadi B.A., Axon L., Martinovic I. 99 % false positives: a qualitative study of SOC analysts' perspectives on security alarms. *31st USENIX Security Symposium*. Boston, USENIX Association, 2022, pp. 2783–2800.

7. Shahjee D., Ware N. Integrated network and Security Operation Center: a systematic analysis. *IEEE Access*, 2022, vol. 10, pp. 27881–27898.

8. Tanenbaum A.S., Steen M. van. *Raspredelennye sistemy. Printsipy i paradigm* [Distributed systems: principles and paradigms]. St. Petersburg, Piter Publ., 2003. 876 p. (In Russian).

9. Tsvetkov V.Ya., Alpatov A.N. Problemy raspredelennykh sistem [Problems of distributed systems]. *Perspektivy nauki i obrazovaniya = Perspectives of Science and Education*, 2014, no. 6 (12), pp. 31–36.

10. Ob ustanovke konveyyerov obrabotki sobytiy [About installing event processing pipelines]. *Positive Technologies. Dokumentatsiya po produktam* [Positive Technologies. Product documentation]. Available at: https://help.ptsecurity.com/projects/siem/latest/ru-RU/help/3690716683 (accessed 01.12.2023).

11. KOMRAD Enterprise SIEM. *Eshelon. Kompleksnaya bezopasnost'* [Echelon. Information security]. Available at: https://npo-echelon.ru/production/65/11793 (accessed 01.12.2023).

12. RuSIEM. (In Russian). Available at: https://rusiem.com/ru/products/rusiem (accessed 01.12.2023).

13. Durnov R.V. Model' raspredelennoi vychislitel'noi seti [Distributed computing network model]. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki = News of the Tula state university. Technical sciences*, 2022, no. 9, pp. 151–153.

14. Dudnikova A.I. Development of a network traffic monitoring system based on Flow protocols. *Molodezh'. Obshchestvo. Sovremennaya nauka, tekhnika i innovatsii = Youth. Society. Modern science, technologies & innovations*, 2021, no. 20, pp. 193–195.

15. Kim S., Park K.-J., Lu C. A survey on network security for cyber–physical systems: from threats to resilient design. *IEEE Communications Surveys & Tutorials*, 2022, vol. 24 (3), pp. 1534–1573. DOI: 10.1109/COMST.2022.3187531.

16. Martins I., Resende J.S., Sousa P.R., Silva S., Antunes L., Gama J. Host-based IDS: a review and open issues of an anomaly detection system in IoT. *Future Generation Computer Systems*, 2022, vol. 133, pp. 95–113.

17. Formby D., Beyah R. Temporal execution behavior for host anomaly detection in programmable logic controllers. *IEEE Transactions in Information Forensics and Security*, 2020, vol. 15, pp. 1455–1469.

18. Skendžić A., Kovačić B., Balon B. Management and monitoring security events in a business organization – SIEM system. *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*, Opatija, 2022, pp. 1203–1208.

19. Thursday Ehis A.-m. Optimization of security information and event management (SIEM) infrastructures, and events correlation/regression analysis for optimal cyber security posture. *Archives of Advanced Engineering Science*, 2023, pp. 1–10. DOI: 10.47852/bonviewAAES32021068.

20. Biryukov S.A., Dyakov S.A. Primenenie metodiki upravleniya riskami v malykh i srednikh stroitel'nykh organizatsiyakh [Application of risk management techniques in small and medium-sized construction companies]. *Vestnik Akademii znanii = Bulletin of the Academy of Knowledge*, 2021, no. 42 (1), pp. 36–45.

21. Xiong W., Legrand E., Åberg O., Lagerström R. Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling*, 2022, vol. 21 (1), pp. 157–177. DOI: 10.1007/s10270-021-00898-7.

22. FSTEC of Russia. *The methodological document "Methodology for assessing information security threats"* (approved by FSTEC of Russia 05.02.2021, as amended 06.12.2022). (In Russian).

Для цитирования:

Методика организации процесса мониторинга распределенных информационных систем / А.В. Иванов, И.А. Огнев, И.В. Никрошкин, Ю.А. Попова // Безопасность цифровых технологий. – 2023. – № 4 (111). – С. 9–23. – DOI: 10.17212/2782-2230-2023-4-9-23.

For citation:

Ivanov A.V., Ognev I.A., Nikroshkin I.V., Popova Yu.A. Metodika organizatsii protsessa monitoringa raspredelennykh informatsionnykh sistem [Methodology for organizing the process of monitoring of distributed information systems]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 4 (111), pp. 9–23. DOI: 10.17212/2782-2230-2023-4-9-23.