УДК 004.056 Вестник УрФО № 4(54) / 2024, с. 22–29

Белоногов А. С., Будник М. Г., Мельников А. В. DOI: 10.14529/secur240403

ИНСТРУМЕНТАЛЬНАЯ СРЕДА РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье исследовано взаимодействие открытой системы IRP, разрабатываемой международным сообществом, с межсетевыми экранами российского производства. На основе функций системы «TheHive» реализован функционал по блокированию атак с внешнего периметра. Представлен алгоритм модуля взаимодействия с межсетевыми экранами для предотвращения компьютерных атак, для разработки которого использован язык Python, в частности, модуль textFSM. Результатом является IRP-система с реализованной пользовательской функцией реагирования, которая может послужить технологической основой в работе Центра обеспечения безопасности (SOC).

Ключевые слова: *IRP-система, SOC, информационная безопасность, кибератака, реагирование на инциденты, центр обеспечения безоапасности.*

Belonogov A. S., Budnik M. G., Melnikov A. V.

INFORMATION SECURITY INCIDENT RESPONSE TOOLING ENVIRONMENT

The article examines the interaction of an open IRP system developed by the international community with Russian-made firewalls. Based on the functions of the "TheHive" system, the functionality for blocking attacks from the external perimeter is implemented. The algorithm of the module for interaction with firewalls to prevent computer attacks is presented, for the development of which the Python language is used, in particular, the textFSM module. The result is an IRP system with an implemented user response function, which can serve as a technological basis for the work of the Security Center (SOC).

Keywords: *IRP system, SOC, information security, cyberattack, incident response, security operations center.*

Введение.

Киберпреступления ежегодно приносят серьезный урон государственным и коммерческим организациям. Согласно [1] за 2023 год ущерб от IT-преступлений превысил в РФ 156 млрд. руб., в то же время по оценке [2] в США заявленный ущерб за тот же период составил 12,5 млрд. долларов США. С ростом объема и ценности обрабатываемых данных соответствующим образом должны развиваться и способы защиты информации от кибератак. Обеспечение информационной безопасности – это непрерывный процесс, задача с неснижающейся актуальностью. Чтобы решать ее с достаточным уровнем оперативности и качества при определенных размерах компании целесообразным может стать создание ведомственного или привлечение стороннего Центра обеспечения безопасности (Security Operation Center, SOC). В компании такой центр обеспечивает непрерывную защиту организации от киберугроз. Центр обеспечения безопасности в своей деятельности опирается на различные технические средства (рис.1), обеспечивающие его функциональность, однако обязательными можно считать базовые средства мониторинга и реагирования. [3, 4]

При этом отмечается постоянно растущая нагрузка на [5,6] специалистов SOC и рутинный характер работы [7], приводящий, в том числе, к высокой текучести кадров. [4] Попытки облегчить и ускорить рутинную работу аналитика SOC проводятся в [5-10], преимущественно с применением технологий искусственного интеллекта. Делать это предполагается, например, за счет автоматизации подготовки плейбуков реагирования на кибератаки [6], или созданию помощника с искусственным интеллектом [5], и прочими способами. В данной работе мы рассмотрим автоматизацию одного из рутинных действий аналитика SOC с применением системы класса IRP.

Системы IRP.

Для автоматизации реагирования на инциденты, совместной работы над расследованием и реагированием на инциденты, построения отчетности применяются системы класса IRP (Incident Response Platform). Данный класс систем позволяет повысить эффективность про-цессов работы над инцидентом. [11]

Перечислим базовые функции IRP-систем:

- регистрация инцидента;
- совместная работа специалистов при реагировании на инцидент;
- эскалация и оповещение;
- интеграция с существующими в компании средствами;
- автоматизированное реагирование на инциденты;
- база знаний;
- отчеты. [12]

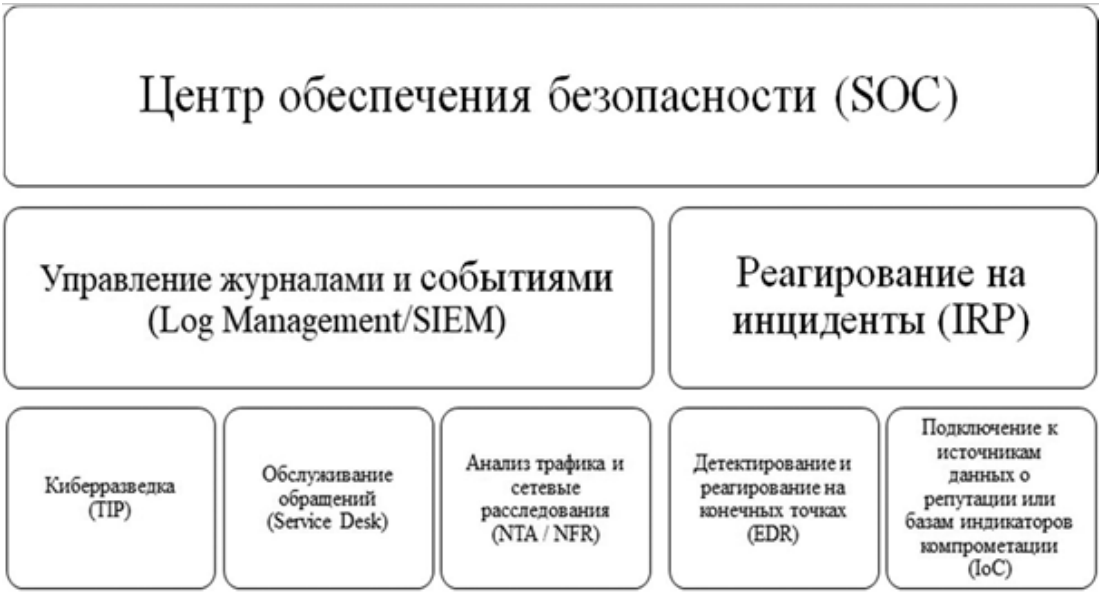

Рис. 1. Функциональная структура центра обеспечения безопасности

Таблица 1.

Заявленные интеграции российских производителей IRP-систем с межсетевыми экранами

	Security Vision [13]	**R-Vision SOAR [14]**	**Innostage Orchestrator [15]**
Зарубежные производители межсетевых экранов	Cisco ASA Fortigate Check Point Cisco Firepower Juniper	Не заявлено	Check Point Palo Alto Huawei
Российские производители межсетевых экранов	Не заявлено	Не заявлено	Usergate

Для реализации автоматизированного реагирования на инциденты IRP система должна иметь возможность интегрироваться с существующими в организации средствами защиты информации. При этом обычной ситуацией является использование для целей обеспечения защиты информации нескольких типов продуктов и инструментов от различных производителей. Современные продукты могут работать независимо, и, как правило, имеют собственные механизмы представления данных, не соблюдающие стандартизацию для обмена данными. [10]

Так, например, коммерческие IRP от российских производителей заявляют поддержку российских средств защиты информации типа межсетевой экран в довольно ограниченном объеме, что отображено в Таблице 1.

Система с открытым исходным кодом TheHive во взаимодействии с продуктом той же команды разработчиков Cortex позволяет автоматизировать запуск определенных функций. В системе TheHive этот процесс реализован через механизм запуска анализаторов (Analyzer) и ответчиков (Responder). Подобный функционал может быть использован командой SOC для прерывания выявленной вредоносной деятельности путем блокирования сетевого взаимодействия с указанным внешним IP-адресом на пограничном межсетевом экране.

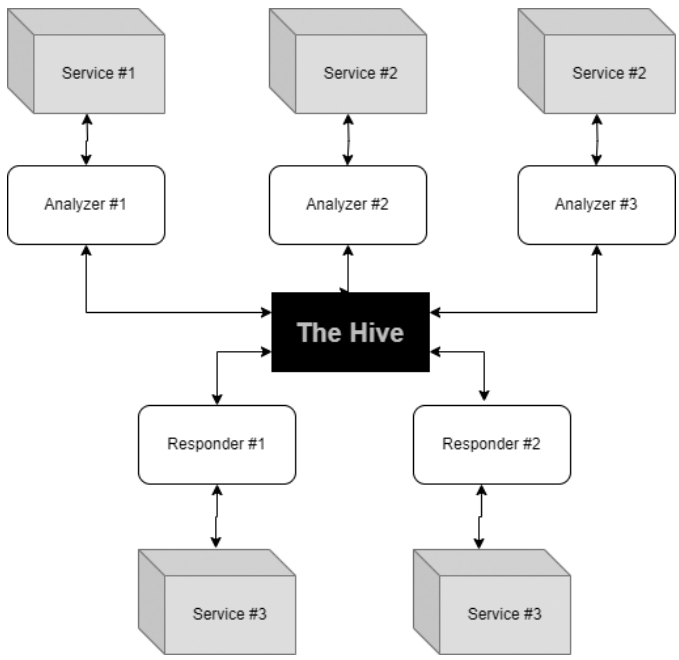

Рис. 2. Структурная схема TheHive.

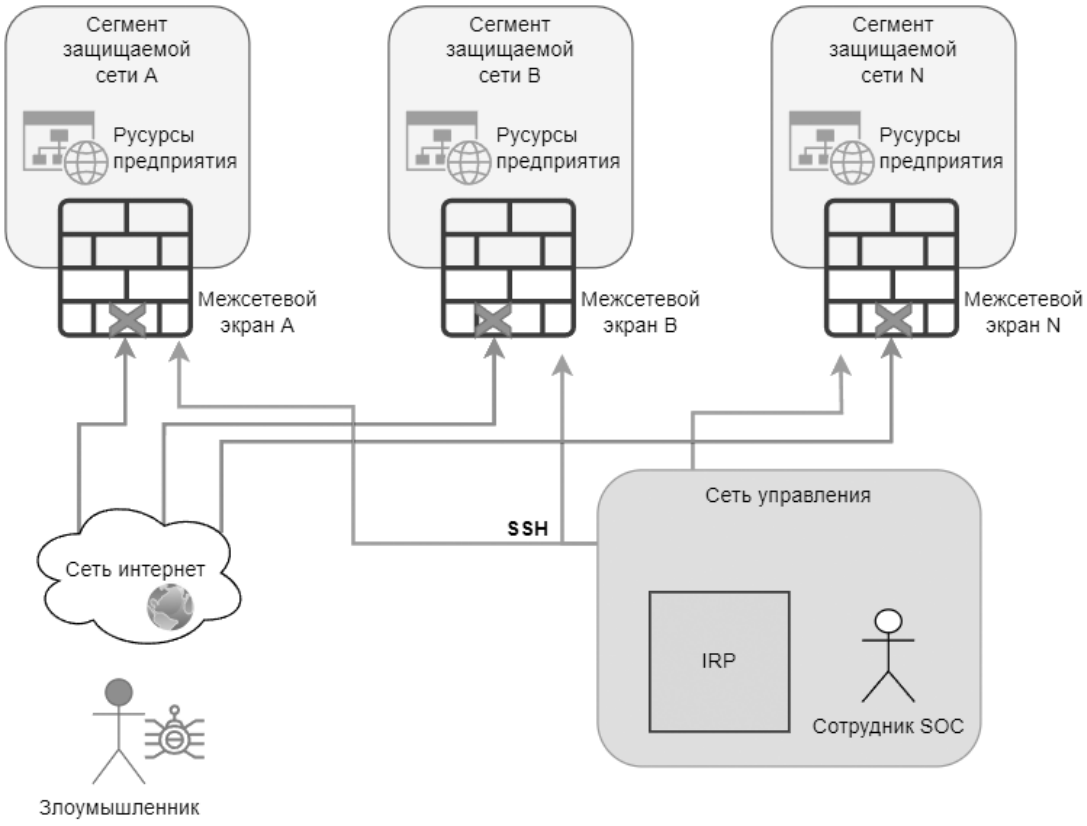

Рис. 3. Общая схема сетевых воздействий на межсетевые экраны при входящей атаке на ресурсы

Разработчики системы TheHive опубликовали руководство для создания собственных функций реагирования (ответчиков), что позволяет самостоятельно продумать и реализовать возможные способы решения задач защиты в конкретной инфраструктуре (рис. 2). [16].

Реализация блокировки атакующих IP-адресов.

В рамках рассматриваемого примера необходимо упомянуть об особенностях атак с внешнего периметра. Как правило наиболее типовыми будут: сканирование с целью выявления открытых сервисов инфраструктуры (разведка), использование в автоматическом режиме скриптов, экс-плуатирующих известные уязвимости, например, SQL-инъекции.

Мерой противодействия таким атакам является добавление правила на пограничный межсетевой экран для блокировки трафика от IP-адреса нарушителя. Необходимость автоматизации таких действий рассматривается как одна из первоочередных в [6]. Потребность усиливается при наличии в обслуживании SOC нескольких сегментов защищаемых компьютерных сетей предприятий.

Рассмотрим блокирование атаки на межсетевом экране российского производства ПАК ViPNet xFirewall 5. Через использование функционала ответчика (Responder) эксперт центра обеспечения безопасности может моментально отправить данные атакующего узла для создания блокирую-щего правила на межсетевом экране (рис. 3).

Для конфигурации функции у пользователя необходимо затребовать следующие параметры:

- IP-адрес управления межсетевым экраном;
- порт управления межсетевого экрана;
- пользователь межсетевого экрана;
- пароль пользователя межсетевого экрана;
- пароль перехода в привилегированный режим.

Для создания ответчика с применением языка Python необходимо подготовить 3 файла: файл с кодом алгоритма на языке Python, файл с перечислением всех зависи-

мостей, используемых в коде программы, и файл взаимодействия со службой, описывающий в формате JSON ключевые параметры взаимодействия с функцией.

Приведем примеры параметров, обязательных для заполнения в вышеуказанном JSON-файле:

• DataTypeList – список типов данных TheHive, поддерживаемых ответчиком;

• Command – это относительный путь к исполняемому файлу програм-мы, в нашем случае: IPBlock/ipblock.py;

• ConfigurationItems – список элементов конфигурации, предназначенных для установки всех переменных ответчиков непосредственно в пользовательском интерфейсе Cortex.

Особенностью рассматриваемого межсетевого экрана является отсутствие опубликованных API для взаимодействия с его конфигурацией. Вследствие чего работа пользовательского кода основана на подключении к консоли управления ПАК по протоколу SSH. Дальнейшая работа автоматической конфигурации производится посредством анализа структурированного вывода (рис. 4). С целью проверки результатов выполнения функции Responder весь вывод, полученный от межсетевого экрана анализируется при помощи модуля textFSM. [17]

Заключение

Приведенная реализация сервиса блокирования целена-правленных атак на инфраструктуру извне расширила возможности системы TheHive, позволяя увеличить скорость реакции команды Центра обеспечения безопасности на киберугрозы. Благодаря принципу открытости исследуемой IRP-системы, становится возможно произвести настройку и интеграцию практически в любой конфигурации компьютерной сети, что, в свою очередь, является серьезным подспорьем для создания ведомственного Центра обеспечения безопасности без высоких первоначальных затрат. Для повышения качества и эффективности реагирования на киберугрозы актуальной задачей является разработка ответчиков (Responders), способных взаимодействовать со средствами технической защиты информации российского производства.

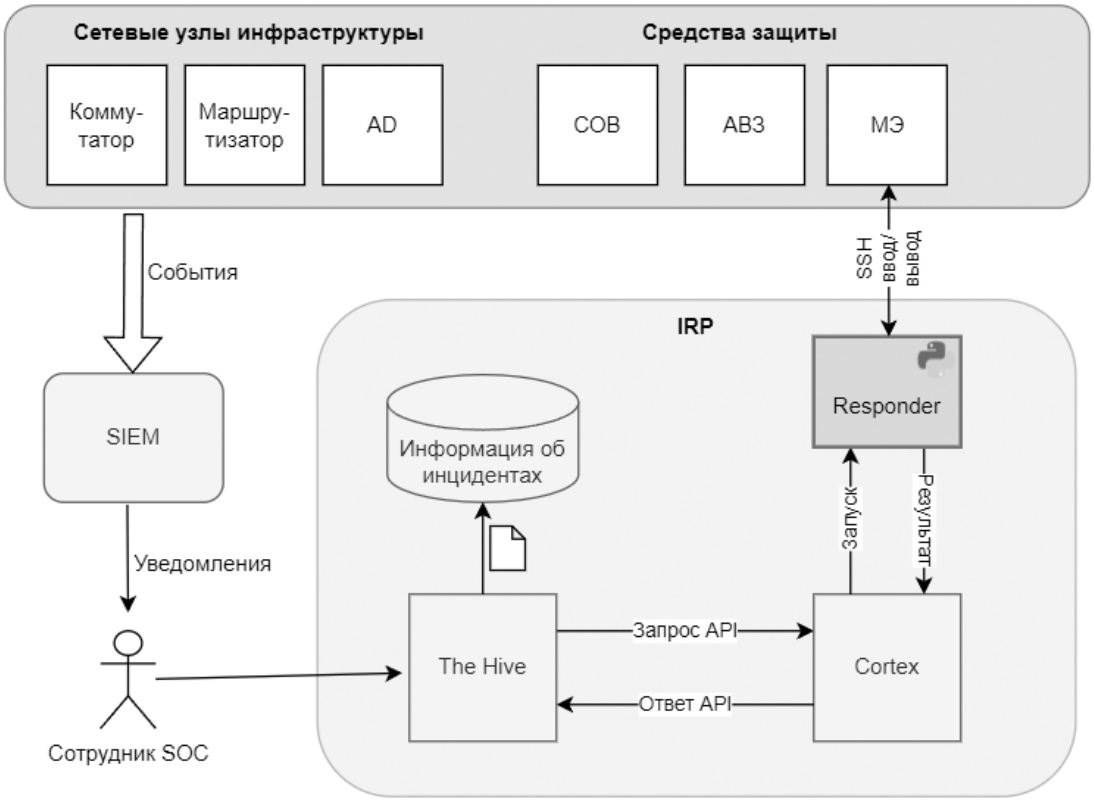

Рис. 4. Схема работы сотрудника SOC с применением TheHive и разработанного ответчика

Литература

1. Расширенное заседание коллегии МВД 2 апреля 2024 года, 15:00 Москва. Стенограмма доклада В.В. Путина. Режим доступа: http://kremlin.ru/events/president/news/73770 (дата обращения 07.11.2024 г.)

2. I.C.C. Center. Internet Crime Complaint Center. Режим доступа: https://www.ic3.gov/ (дата обращения 01.11.2024 г.)

3. Очередько А.Р. Исследование IRP-систем на основе анализа механизмов реагирования на инциденты информационной безопасности / А. Р. Очередько, Д.А. Бачманов, М.М. Путято, А. С. Макарян // Прикаспийский журнал: управление и высокие технологии. – 2021. – № 1. – С. 74–82.

4. Manfred Vielberth, Fabian Böhm, Ines Fichtinger, Günther Pernul Se-curity Operations Center: A Systematic Study and Open Challenges // IEEE Access (Volume: 8), P. 227756–227779 – 2020 – DOI: 10.1109/ACCESS.2020.3045514 – Режим доступа: https://ieeexplore.ieee.org/document/9296846

5. Scott Freitas, Amir Gharib, Jovan Kalajdjieski, Robert McCann AI-Driven Guided Response for Security Operation Centers with Microsoft Copilot for Security – 2024 – DOI: 10.48550/arXiv.2407.09017 – Режим доступа: https://arxiv.org/abs/2407.09017

6. Ryuta Kremer, Prasanna N. Wudali, Yuval Elovici, Asaf Shabtai, Satoru Momiyama, Toshinori Araki, Jun Furukawa, IC-SECURE: Intelligent System for Assisting Security Experts in Generating Playbooks for Automated Incident Response – DOI: 10.48550/arXiv.2311.03825 – Режим доступа: https://arxiv.org/pdf/2311.03825

7. Andreas U. Schmidt, Sven Knudsen, Tobias Niehoff, and Klaus Schwietz Planning Distributed Security Operations Centers in Multi-Cloud Landscapes: A Case Study – 2023 – DOI: 10.48550/arXiv.2303.03141 – Режим доступа: https://arxiv.org/abs/2303.03141

8. PeiYu Tseng, ZihDwo Yeh, Xushu Dai, Peng Liu Using LLMs to Au-tomate Threat Intelligence Analysis Workflows in Security Operation Centers // JOURNAL OF LATEX CLASS FILES, Vol. 18, No. 9 – 2020 – DOI: 10.48550/arXiv.2407.13093 – Режим доступа: https://arxiv.org/pdf/2407.13093

9. Hari Hayagreevan, Souvik Khamaru Security of and by Generative AI platforms // Whitepaper February 2024 – DOI: 10.48550/arXiv.2410.13899 – Режим доступа: https://arxiv.org/pdf/2410.13899

10. Johnson Kinyua, Lawrence Awuah AI/ML in Security Orchestration, Automation and Response: Future Research Directions // Intelligent Automation & Soft Computing 2021 Vol.28, No.2, P. 527-545 – 2021 – DOI: 10.32604/iasc.2021.016240 – Режим доступа: https://www.techscience.com/iasc/v28n2/42057/pdf

11. Обзор рынка платформ реагирования на инциденты (IRP) в России. – 2018. – Режим доступа: https://www.anti-malware.ru/analytics/Market_Analysis/incident-response-platforms-irp-in-russia, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 26.10.2023 г.)

12. Бесплатная IRP-система своими силами: опыт использования платформы с открытым кодом The Hive. – 2019. – Режим доступа: https://www.anti-malware.ru/practice/solutions/free-IRP-on-your-own, свобод-ный. – Заглавие с экрана. – Яз. рус. (дата обращения: 27.10.2023 г.)

13. Опросный лист Security Vision для подготовки ТКП. Режим доступа: https://www.securityvision.ru/downloads/%D0%9E%D0%BF%D1%80%D0%BE%D1%81%D0%BD%D1%8B%D0%B9%20%D0%BB%D0%B8%D1%81%D1%82%20Security%20Vision.xlsx (дата обращения 21.06.2024)

14. Опросный лист R-Vision SOAR. Режим доступа: https://rvision.ru/blog-posts/usloviya-priobreteniya-po (дата обращения 21.06.2024)

15. Innostage Orchestrator Система управляющих воздействий. Режим доступа: https://inno-orch.ru/ – Заглавие с экрана. (дата обращения 24.06.2024)

16. The Hive-Project. – 2020. – Режим доступа: https://github.com/TheHive-Project/TheHive, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 24.10.2023 г.)

17. TextFSM. – 2023. – Режим доступа: https://github.com/google/textfsm/wiki/TextFSM, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 26.10.2023 г.).

References

1. Rasshirennoye zasedaniye kollegii MVD 2 aprelya 2024 goda, 15:00 Moskva. Stenogramma doklada V.V. Putina. Rezhim dostupa: http://kremlin.ru/events/president/news/73770 (data obrashcheniya 07.11.2024 g.)

2. I.C.C. Center. Internet Crime Complaint Center. Rezhim dostu-pa: https://www.ic3.gov/ (data obrashcheniya 01.11.2024 g.)

3. Ochered'ko A.R. Issledovaniye IRP-sistem na osnove analiza mekha-nizmov reagirovaniya na intsidenty informatsionnoy bezopasnosti / A. R. Ochered'ko, D.A. Bachmanov, M.M. Putyato, A. S. Makaryan // Pri-kaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii. – 2021. – № 1. – S. 74–82.

4. Manfred Vielberth, Fabian Böhm, Ines Fichtinger, Günther Pernul Se-curity Operations Center: A Systematic Study and Open Challenges // IEEE Access (Volume: 8), P. 227756–227779 – 2020 – DOI: 10.1109/ACCESS.2020.3045514 – Rezhim dostupa: https://ieeexplore.ieee.org/document/9296846

5. Scott Freitas, Amir Gharib, Jovan Kalajdjieski, Robert McCann AI-Driven Guided Response for Security Operation Centers with Microsoft Copilot for Security – 2024 – DOI: 10.48550/arXiv.2407.09017 – Rezhim dostupa: https://arxiv.org/abs/2407.09017

6. Ryuta Kremer, Prasanna N. Wudali, Yuval Elovici, Asaf Shabtai, Satoru Momiyama, Toshinori Araki, Jun Furukawa, IC-SECURE: Intelligent System for Assisting Security Experts in Generating Playbooks for Automated Incident Response – DOI: 10.48550/arXiv.2311.03825 – Rezhim dostupa: https://arxiv.org/pdf/2311.03825

7. Andreas U. Schmidt, Sven Knudsen, Tobias Niehoff, and Klaus Schwietz Planning Distributed Security Operations Centers in Multi-Cloud Landscapes: A Case Study – 2023 – DOI: 10.48550/arXiv.2303.03141 – Rez-him dostupa: https://arxiv.org/abs/2303.03141

8. PeiYu Tseng, ZihDwo Yeh, Xushu Dai, Peng Liu Using LLMs to Au-tomate Threat Intelligence Analysis Workflows in Security Operation Centers // JOURNAL OF LATEX CLASS FILES, Vol. 18, No. 9 – 2020 – DOI: 10.48550/arXiv.2407.13093 – Rezhim dostupa: https://arxiv.org/pdf/2407.13093

9. Hari Hayagreevan, Souvik Khamaru Security of and by Generative AI platforms // Whitepaper February 2024 – DOI: 10.48550/arXiv.2410.13899 – Rezhim dostupa: https://arxiv.org/pdf/2410.13899

10. Johnson Kinyua, Lawrence Awuah AI/ML in Security Orchestration, Automation and Response: Future Research Directions // Intelligent Automation & Soft Computing 2021 Vol.28, No.2, P. 527-545 – 2021 – DOI: 10.32604/iasc.2021.016240 – Rezhim dostupa: https://www.techscience.com/iasc/v28n2/42057/pdf

11. Obzor rynka platform reagirovaniya na intsidenty (IRP) v Rossii. – 2018. – Rezhim dostupa: https://www.anti-malware.ru/analytics/Market_Analysis/incident-response-platforms-irp-in-russia, svobodnyy. – Zaglaviye s ekrana. – Yaz. rus. (data obrashcheniya: 26.10.2023 g.)

12. Besplatnaya IRP-sistema svoimi silami: opyt ispol'zovaniya platformy s otkrytym kodom The Hive. – 2019. – Rezhim dostupa: https://www.anti-malware.ru/practice/solutions/free-IRP-on-your-own, svobodnyy. – Zaglaviye s ekrana. – Yaz. rus. (data obrashcheniya: 27.10.2023 g.)

13. Oprosnyy list Security Vision dlya podgotovki TKP. Rezhim dostupa: https://www.securityvision.ru/downloads/%D0%9E%D0%BF%D1%80%D0%BE%D1%81%D0%BD%D1%8B%D0%B9%20%D0%BB%D0%B8%D1%81%D1%82%20Security%20Vision.xlsx (data obrashcheniya 21.06.2024)

14. Oprosnyy list R-Vision SOAR. Rezhim dostupa: https://rvision.ru/blog-posts/usloviya-priobreteniya-po (data obrashcheniya 21.06.2024)

15. Innostage Orchestrator Sistema upravlyayushchikh vozdeystviy. Rez-him dostupa: https://innoorch.ru/ – Zaglaviye s ekrana. (data obrashche-niya 24.06.2024)

16. The Hive-Project. – 2020. – Rezhim dostupa: https://github.com/TheHive-Project/TheHive, svobodnyy. – Zaglaviye s ekrana. – Yaz. angl. (data obrashcheniya: 24.10.2023 g.)

17. TextFSM. – 2023. – Rezhim dostupa: https://github.com/google/textfsm/wiki/TextFSM, svobodnyy. – Zaglaviye s ekrana. – Yaz. angl. (data obrashcheniya: 26.10.2023 g.).

Белоногов Александр Сергеевич, руководитель центра сетевых технологий и телекоммуникаций, автономное учреждение Ханты-Мансийского автономного округа – Югры «Югорский научно-исследовательский институт информационных технологий». 628011, г. Ханты-Мансийск, ул. Мира, 151. E-mail: BelonogovAS@uriit.ru

Будник Максим Геннадьевич, начальник отдела развития и автоматизации ИТ инфраструктуры центра сетевых технологий и телекоммуникаций, автономное учреждение Ханты-Мансийского автономного округа – Югры «Югорский научно-исследовательский институт информационных технологий». 628011, г. Ханты-Мансийск, ул. Мира, 151. E-mail: BudnikMG@uriit.ru

Мельников Андрей Витальевич, доктор технических наук, профессор, директор, автономное учреждение Ханты-Мансийского автономного округа – Югры «Югорский научно-исследовательский институт информа-ционных технологий». 628011, г. Ханты-Мансийск, ул. Мира, 151. E-mail: MelnikovAV@uriit.ru

Belonogov Alexander Sergeevich, Head of the Center for Network Technologies and Telecommunications, Ugra Research Institute of Information Technologies. 628011, Khanty-Mansiysk, Mira str., 151. Email: Belonogo-vAS@uriit.ru

Budnik Maxim Gennadievich, Head of the IT Infrastructure Development and Automation Department of the Center for Network Technologies and Telecommunications, Ugra Research Institute of Information Technologies. 628011, Khanty-Mansiysk, Mira str., 151. Email: BudnikMG@uriit.ru

Melnikov Andrey Vitalievich, Doctor of Technical Sciences, Professor, Director, Ugra Research Institute of Information Technologies. 628011, Khanty-Mansiysk, Mira str., 151. Email: MelnikovAV@uriit.ru