ШКОЛА МОЛОДОГО УЧЕНОГО

УДК 004.056
DOI: 10.18469/ikt.2025.23.1.12

МОДЕЛЬ ОЦЕНКИ КОМПРОМЕТАЦИИ СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ ЭЛЕМЕНТОВ УПРАВЛЕНИЯ ЗНАНИЯМИ

Золотарев В.В.[1], Трофимычев И.И.[2]
[1]Сибирский государственный университет науки и технологий им. академика М.Ф. Решетнева, Красноярск, РФ
[2]Самарский государственный технический университет, Самара, РФ
E-mail: amida.2@yandex.ru, mr.trofimychev@mail.ru

В условиях роста числа и сложности кибератак традиционные методы информационной безопасности теряют свою эффективность. Искусственный интеллект, социальный инжиниринг, обфускации атак – для своевременного обнаружения и реагирования на эти угрозы важно не только вовремя идентифицировать угрозу, но и правильно оценить ее критичность, а также ее роль как элемента более комплексной атаки. В данной работе предлагается модель интеллектуальной системы защиты информации, которая будет включать в себя двухступенчатый подход: сначала на основе существующего предприятия создается граф инфраструктуры, который затем обогащается при помощи онтологии предметной области до графа знаний, позволяя собрать в одной структуре как детальную информацию о защищаемой системе и существующих угрозах, так и более абстрактную информацию о взаимоотношениях между объектами. Данный подход позволяет находить более сложные корреляции между событиями и выстраивать общий план сценария атаки.

Ключевые слова: *информационная безопасность, событие информационной безопасности, графы знаний, интеллектуальные системы, управление инцидентами, оценка уязвимостей*

Введение

Одним из ключевых факторов, обеспечивающих способность компании поддерживать высокий уровень защиты своей инфраструктуры в сфере информационной безопасности, является возможность оперативно и всесторонне собирать и анализировать данные о состоянии системы и происходящих в ней инцидентах. Это позволяет не только глубоко исследовать текущие угрозы, но и формировать основу для точного анализа и эффективного реагирования на подобные события в будущем. На настоящий момент наиболее эффективным способом решения данной задачи является связка из SIEM (Security Information and Event Management) + SOAR (Security Orchestration, Automation and Response) систем, однако она имеет некоторые значительные недостатки:

– ограниченное понимание контекста;
– высокая потребность в экспертной оценке;
– сложная настройка системы в каждом индивидуальном случае;
– ухудшение работы при атаке с нескольких сторон, невозможность разглядеть «глобальную картину», уязвимость к обфускации атак.

Для того, чтобы компенсировать эти недостатки в данной работе предлагается модель интеллектуальной системы защиты информации (ИСЗИ) [1], которая позволяет работать с системой одновременно на двух уровнях: первый – топологический – будет использовать сетевой граф для определения физической связи объектов друг с другом, в то время как второй – семантический – будет использовать базу знаний для определения логической связи объектов друг с другом с точки зрения знаний предметной области. Данный подход позволит выйти за рамки привычной детекции инцидентов как отдельных объектов информационной безопасности и перейти к решению задач более общего порядка, таких как:

– определение потенциальных сценариев атаки относительно произошедших инцидентов;
– идентификация группы злоумышленников, ответственных за совершение определенного набора инцидентов;
– прогнозирование целевого узла атаки по уже совершенным инцидентам;
– идентификация атак с обфускацией инцидентов.

Несмотря на то, что использование графов является классическим подходом в сфере информационной безопасности [2], управление знаниями с использованием онтологий предметных областей является сравнительно новым решением в области информационных технологий [3–10].

Базовые элементы системы. Граф сети

Для начала определим, что мы понимаем под сетевым графом первого уровня, т.е. опишем, что считается компонентами системы, и составим на основе этой информации граф системы. Итак, пусть у нас имеется ориентированный граф системы $G(N,E)$, где N – множество элементов системы, E – множество связей между ними. В таком случае множество N в первом приближении будет равно множеству $N_{ву}$, $N_{ву}$ – множество вычислительных устройств системы (рабочие станции, сервера, коммутаторы, маршрутизаторы и так далее). Соответственно в этом случае множество E будет представлять из себя множество $E_{ву}$, описывающее все возможные связи между устройствами в сети (здесь учитываются как связи через локальную сеть, так и через внешнюю) (рисунок 1).

Несмотря на то, что вычислительные устройства составляют часть любой современной инфраструктуры, современные тенденции стратегий злоумышленников говорят о том, что наиболее уязвимым звеном в любой защищаемой инфраструктуре все еще является человек. Для того, чтобы учесть данный фактор, расширим множество N, добавив в него элементы множества N_C, где N_C – множество сотрудников компании, имеющих возможность взаимодействовать с данной инфраструктурой. Далее соответствующим образом расширим множество E, добавив в него элементы E_C, где E_C – возможность сотрудников контактировать между собой и вычислительными устройствами в сети. Здесь так же нельзя забывать о том, что сотрудники могут взаимодействовать с вычислительными не только напрямую, используя специальные интерфейсы (такие как мышь, экран, клавиатура), но и при помощи вспомогательных элементов, таких как внешние запоминающие устройства (ВЗУ) (рисунок 2).

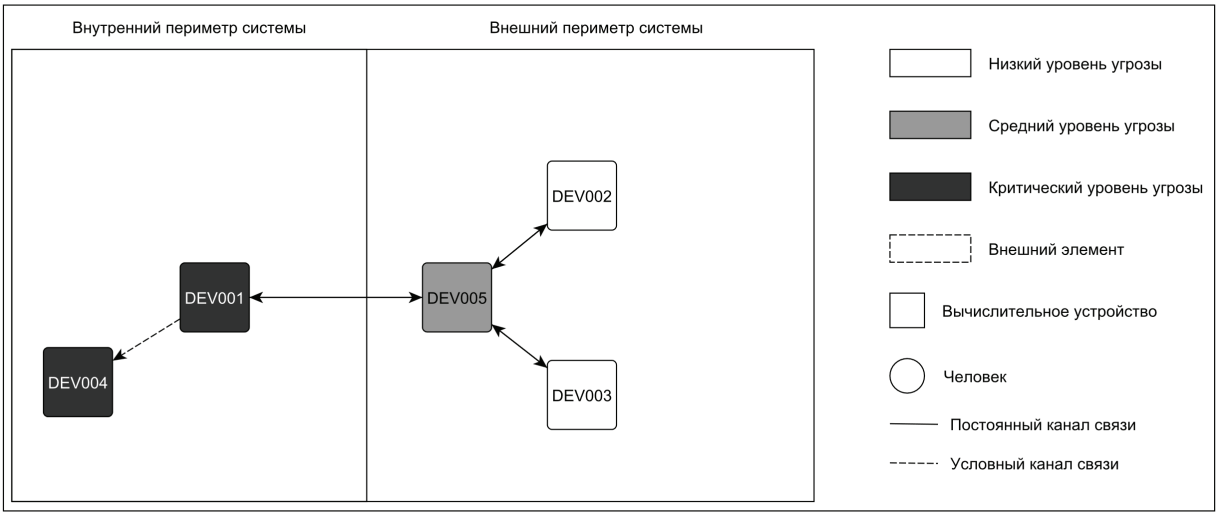

Рисунок 1. Граф системы в первом приближении

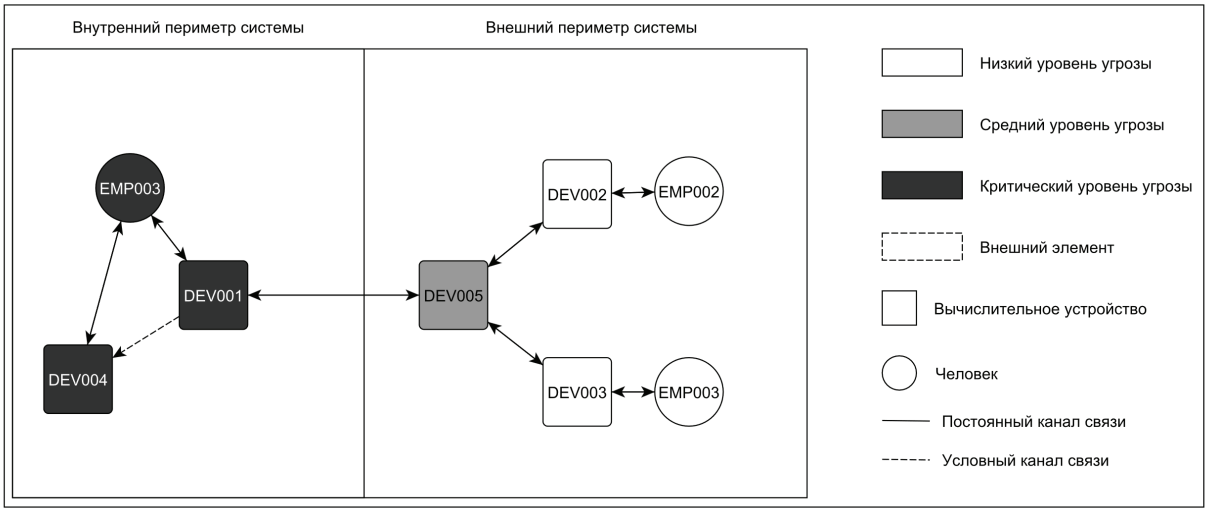

Рисунок 2. Граф системы, включающий в себя сотрудников

Наконец, для корректного отражения действий злоумышленников следует ввести фиктивные внешние узлы $N_ф$ и соответствующие им связи $E_ф$. Следует также учесть, что некоторые ребра в графе G могут обладать свойством условности, т.е. появляться и исчезать в графе в зависимости от определенных условий (рисунок 3).

Обогащение графа при помощи базы знаний. Граф знаний

Для перехода от структурного представления инфраструктуры к контекстно-ориентированному анализу система дополняется семантическим слоем – базой знаний D, интегрируемой с сетевым графом. Этот двухуровневый подход позволяет не только отображать физические связи между объектами, но и моделировать их функциональные, ролевые и операционные взаимоотношения, что критически важно для прогнозирования угроз и оценки уязвимостей. В зависимости от типа элемента сетевого графа информация о нем может различаться, но при этом она должна отражать основные характеристики объекта. Предполагаемый список характеристик с учетом имеющегося сетевого графа может включать в себя следующие элементы:

1. Люди (сотрудники):

– уникальные идентификаторы (ID, биометрические данные);

– привилегии (доступ к устройствам, управление учетными записями, работа с программным обеспечением (ПО));

– контекст активности (расписание работы, шаблоны поведения, должность, связь с отделами).

2. Вычислительные устройства:

– уникальный идентификатор устройства (серийные номера компонентов);

– параметры устройства в сети (MAC-адрес, IPv4/IPv6);

– техническая спецификация (центральный процессор, оперативное запоминающее устройство, дисковое пространство, тип устройства);

– программная среда (операционная система, установленное ПО, сетевые службы);

– защита системы (наличие EDR/XDR-решений, журналы аудита, доступ к корпусу устройства).

3. Связи между вершинами графа:

– тип связи (сетевая, логическая, социальная);

– атрибуты безопасности.

Информация, представленная в базе знаний, будет использоваться для сопоставления с характерными особенностями сценариев, чтобы своевременно и точно оценивать вероятность компрометации системы, а также выявлять наиболее критичные узлы с точки зрения информационной безопасности.

Базовые элементы атаки на систему

Рассмотрим потенциальную атаку на любую инфраструктуру. Минимальным элементом атаки на систему является инцидент информационной безопасности. Инцидентом информационной безопасности (ИБ), в свою очередь, является нежелательное событие, компрометирующее один или несколько элементов системы.

В то время как компрометация вычислительных устройств и каналов взаимодействия между ними является достаточно изученной областью и данную информацию можно получать, используя специальные системы управления событиями и анализ траффика сети, в свою очередь, определение компрометации узла, представляющего из себя сотрудника, является достаточно нетриви-

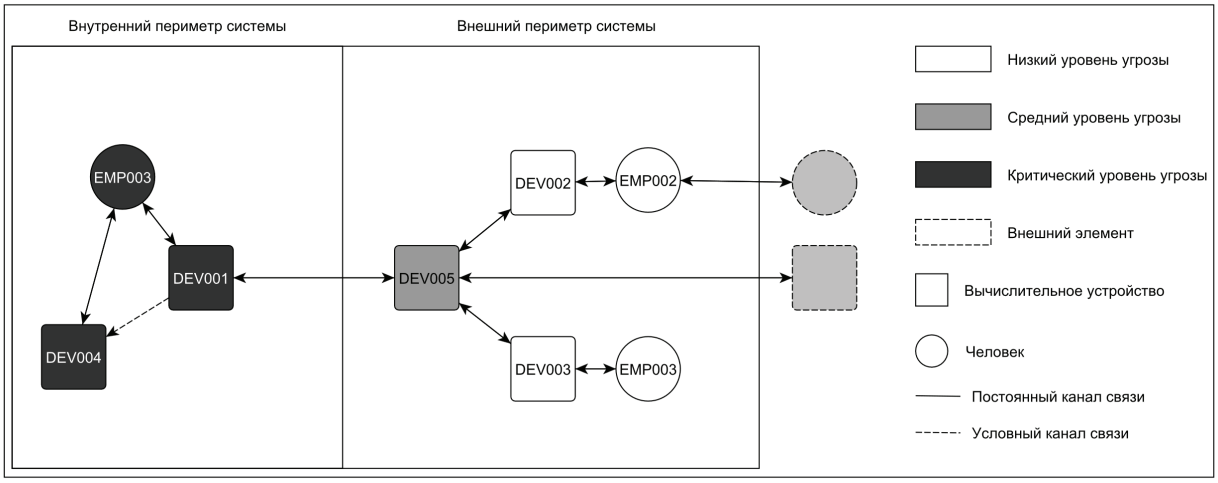

Рисунок 3. Финальная версия графа

альной задачей [11]. Тем не менее, для данного исследования можно определить компрометацию сотрудника следующим образом: при работе человека с вычислительным устройством при помощи специальной системы его показатели (движение глаз, скорость работы, мимика и т.д.) и в случае превышения ими заранее заданных показателей или выполнения действий, нехарактерных для сотрудника и рабочего процесса (открытые лишнего порта, изменение параметров работы системы и т.д.), то делается вывод о компрометации как самого узла, представляющего сотрудника, так и всех связанных с ним ребер.

Определив понятие компрометации, можно сформулировать более точное определение атаки на систему. Сам по себе инцидент ИБ хоть и может представлять угрозу для системы, но обычно все же является составным элементом уже более сложного элемента – сценария атаки. Сценарий атаки представляет из себя последовательность действий злоумышленников, несущую в себе определенную цель – чаще всего добиться компрометации конкретного элемента системы, либо всей системы в целом. С точки зрения описанной модели сценарий атаки представляет из себя множество инцидентов ИБ, которые должны быть связаны с определенными элементами системы, причем некоторые из них должны произойти в строго определенном порядке (рисунок 4).

В рамках описываемой задачи будем считать, что множество всех потенциально существующих сценариев атаки содержится в отдельно хранимой базе знаний Attack Scenario (*AS*), доступной для постоянного взаимодействия с системой. Примером такой базы знаний можно считать матрицу ATT&CK [12].

Схема взаимодействия элементов модели

Суммируя все вышесказанное, можем утверждать, что математическая модель инфраструктуры *GI* представляет из себя набор следующих структур:

1. Ориентированный сетевой граф инфраструктуры *G*.
2. База знаний информационной безопасности *D*.
3. Список инцидентов информационной безопасности *I*, произошедших с системой с начала процесса моделирования.
4. База знаний *A*S, включающая в себя информацию о всех известных на данных момент сценариях атаки.

На этапе построения модели информация о графе *G* обогащается информацией из базы знаний *D*, образуя граф знаний *KG*. Таким образом мы получаем графовое представление инфраструктуры компании, где каждый элемент с одной стороны является элементом сетевой модели, а с другой – экземпляром некоторой структуры из глобальной базы знаний. Такой подход не только расширяет контекстную информацию о каждом узле, но и позволяет оценивать информацию о системе с точки зрения ее «полезности». Далее рассматривается информация об инцидентах *I* и подбираются наиболее вероятные сценарии атаки *AS*. Наконец, ключевым этапом является сопоставление участков графа знаний *KG* и вероятных сценариев атаки *AS* для определения вероятности компрометации системы, а также указания на наиболее уязвимые в конкретной ситуации узлы (схема взаимодействия элементов модели на рисунке 5).

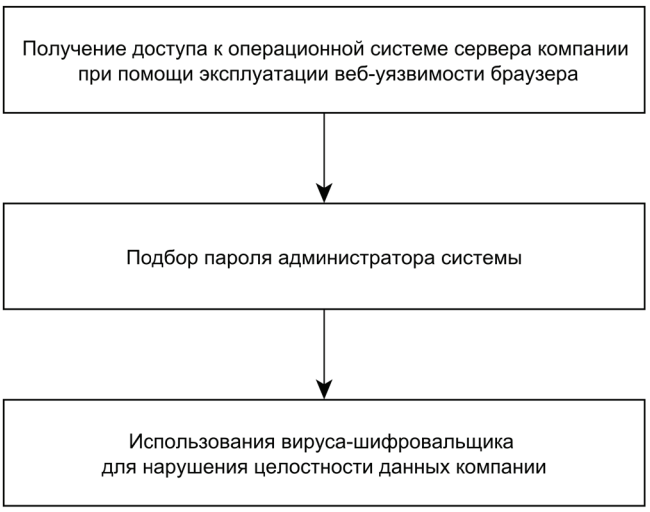

Рисунок 4. Сценарий атаки, состоящий из трех инцидентов

Исходя из представленного выше описания модели, задачу исследования можно сформулировать следующим образом: необходимо определить функцию $p = p(G, I, AS, D)$, возвращающую вероятность компрометации системы при заданных начальных условиях. Предварительно, функция может иметь следующий вид:

$$p = p(G, I, AS, D) = P\left(\bigcup_{i=1}^{|AS^I|} AS_i^I\right);$$

$$AS_i^I = P\left(\bigcup_{j=1}^{|AS_i^I|} ASP_{ij}^I\right);$$

$$ASP_{ij}^I = \frac{\sum_{k=1}^{m} \alpha_{ijk}}{\sum_{k=1}^{n} \alpha_{ijk}},$$

где AS^I – множество событий реализации сценариев атак, для которых релевантен хотя бы один произошедший инцидент из множества I;

ASP_i^I – множество событий реализации вариантов развития сценария атак AS_i^I;

α_{ijk} – коэффициент значимости реализации конкретного инцидента.

Расширение задачи имеет несколько потенциальных векторов развития:

Во-первых, можно модифицировать цель задачи таким образом, чтобы функция p возвращала не только вероятность компрометации системы, но и элемент системы, который с учетом имеющихся заданных условий будет являться ключевым для защиты системы от компрометации.

Во-вторых, задачу можно перевести от статической к динамической: все или некоторые элементы системы (G, I, AS, D) могут изменяться во времени. Данный вопрос предполагает не только то, что элементы могут изменяться в различной последовательности, но и тот факт, что для самих изменений могут требоваться различные периоды времени.

Заключение

В данной работе была рассмотрена модель интеллектуальной системы оценки вероятности компрометации инфраструктуры, основанная на элементах управления знаниями. Данный подход позволяет получить некоторые преимущества по сравнению с классическим подходом SOAR (Security Orchestration, Automation and Response) систем, а именно:

1. Автоматизация процесса: по сравнению с классическими SOAR системами данный подход менее требователен к индивидуальным настройкам под конкретную инфраструктуру.

2. Контекстный анализ данных: использование графа знаний позволяет при помощи единого подхода анализировать данные из различных источников.

3. Интеллектуальный анализ атак: использование элементов управления знаниями дает возможность не только использовать данные из различных источников, но и анализировать их на предмет «полезности», что показывает высокую эффективность во время обфусцированных атак или атак с нескольких сторон.

Тем не менее, перед практической реализацией данной модели необходимо решить несколько важных задач:

– определить точный формат и структуру баз знаний D и AS;

– какие методики покажут наибольшую эффективность для анализа графа знаний KG в контексте поставленной задачи;

– что при использовании данной модели считать за вероятность компрометации системы $p = p(G, I, AS, D)$.

Литература

1. Котенко И.В., Саенко И.Б. Построение системы интеллектуальных сервисов для защиты

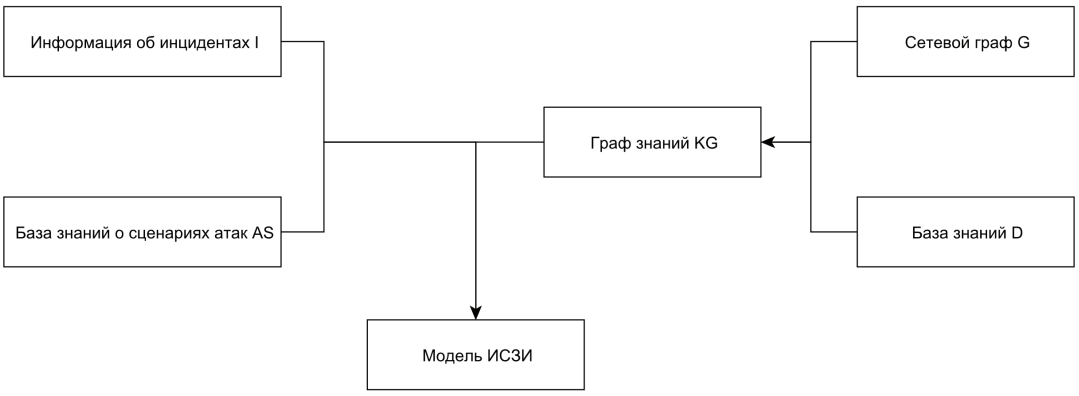

Рисунок 5. Схема взаимодействия элементов модели

информации в условиях кибернетического противоборства // Труды СПИИРАН. 2012. № 3 (22). С. 84–100.
2. Шевцов В.Ю., Правиков Д.И. Применение сетей Петри при моделировании атак на системы АСУ ТП // Вестник современных цифровых технологий. 2022. № 13. С. 32–37.
3. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах / И.В. Котенко [и др.] // Труды СПИИРАН. 2012. № 1 (20). С. 27–56.
4. Malont: An ontology for malware threat intelligence / N. Rastogi [et al.] // Deployable Machine Learning for Security Defense. Cham: Springer International Publishing, 2020. P. 28–44. DOI: 10.1007/978-3-030-59621-7_2
5. Колесникова Д.С., Верещагина Е.А., Гуляев В.Е. Построение онтологической модели для предметной области «Информационная безопасность» // Инженерный вестник Дона. 2023. № 7 (103). С. 81–90.
6. Creating cybersecurity knowledge graphs from malware after action reports / A. Piplai [et al.] // IEEE Access. 2020. Vol. 8. P. 211691–211703. DOI: 10.1109/ACCESS.2020.3039234
7. A survey on cybersecurity knowledge graph construction / X. Zhao [et al.] // Computers and Security. 2024. Vol. 136. P. 103524. DOI: 10.1016/j.cose.2023.103524
8. Касимова А.Р., Сафиуллина Л.Х. Использование цифровых двойников при построении системы безопасности предприятия // Международный форум Kazan Digital Week-2022: сборник материалов Международного форума. Казань: Научный центр безопасности жизнедеятельности, 2022. С. 291–298.
9. Смагин А.А., Полетаев В.С. Алгоритм прогнозирования угроз информационной безопасности // Инфокоммуникационные технологии. 2018. Т. 16, № 2. С. 192–198. DOI: 10.18469/ikt.2018.16.2.06
10. Гребешков А.Ю. Разработка предметно-ориентированной онтологии когнитивной сети доступа стандарта IEEE 802.22 // Инфокоммуникационные технологии. 2018. Т. 16, № 4. С. 379–387. DOI: 10.18469/ikt.2018.16.4.03
11. Разработка системы анализа действий пользователя в информационной среде / Н.Е. Карпова [и др.] // Динамика систем, механизмов и машин. 2020. Т. 8, № 2. С. 114–123.
12. ATT&CK Matrix for enterprise. URL: https://attack.mitre.org/ (дата обращения: 05.02.2025).

Дата поступления 18.02.2025
Дата принятия 18.03.2025

Золотарев Вячеслав Владимирович, заведующий кафедрой безопасности информационных технологий Сибирского государственного университета науки и технологий им. академика М.Ф. Решетнева. 660037, Российская Федерация, г. Красноярск, пр. им. Газеты «Красноярский рабочий», 31. Тел. +7 905 973-80-91. E-mail: amida.2@yandex.ru

Трофимычев Илья Игоревич, преподаватель кафедры электронных систем и информационной безопасности Самарского государственного технического университета. 443100, Российская Федерация, г. Самара, ул. Молодогвардейская, 244. Тел. +7 917 959-51-20. E-mail: mr.trofimychev@mail.ru

UDC 004.056
DOI: 10.18469/ikt.2025.23.1.12

SYSTEM COMPROMISE ASSESSMENT MODEL USING KNOWLEDGE MANAGEMENT ELEMENTS

Zolotarev V.V.[1], Trofimychev I.I.[2]
[1]Reshetnev Siberian State University of Science and Technology, Krasnoyarsk, Russian Federation
[2]Samara State Technical University, Samara, Russian Federation
E-mail: amida.2@yandex.ru, mr.trofimychev@mail.ru

In the context of the increasing number of threats and the complexity of attack methods, traditional approaches to ensuring information security are often not effective enough. This is due both to the limited capabilities of classical anomaly detection methods and insufficient consideration of the context and dynamics of changes in the network environment. In this regard, the task of developing new methods and approaches that allow not only to detect attacks, but also to effectively interpret their nature, as well as detect obfuscated attacks, becomes relevant. This article proposes a model

based on the use of an intelligent information security system, which would expand the capabilities of SOAR systems – it would allow using information coming from the SIEM system not only to search for local vulnerabilities, but also for a comprehensive final goal of the attack vector, including situations of false attacks. For this purpose, it is proposed to use a combined approach based on the use of a knowledge graph model designed by enriching the network graph with a knowledge base about the infrastructure, which would allow finding more complex correlations between individual incidents in the network and larger attack scenarios.

Keywords: *information security, information security event, knowledge graphs, intelligent systems, incident management, vulnerability assessment*

Zolotarev Vyacheslav Vladimirovich, Reshetnev Siberian State University of Science and Technology, 31, Krasnoyarsky Rabochy Avenu, Krasnoyarsk, 660037, Russian Federation; Head of Information Technologies Security Department. Tel. +7 905 973-80-91. E-mail: amida.2@yandex.ru

Trofimychev Ilya Igorevich, Samara State Technical University, 244, Molodogvardeyskaya Street, Samara, 443100, Russian Federation; Teacher of Electronic Systems and Information Security Department. Tel. +7 917 959-51-20. E-mail: mr.trofimychev@mail.ru

References

1. Kotenko I.V., Saenko I.B. Developing the system of intelligent services to protect information in cyber warfare. *Trudy SPIIRAN*, 2012, no. 3 (22), pp. 84–100. (In Russ.)
2. Shevtsov V.Yu., Pravikov D.I. The application of petri nets for modeling attacks on ICS. *Vestnik sovremennykh tsifrovykh tekhnologii*, 2022, no. 13, pp. 32–37. (In Russ.)
3. Kotenko I.V. et al. Application of security information and event management technology for information security in critical. *Trudy SPIIRAN*, 2012, no. 1 (20), pp. 27–56. (In Russ.)
4. Rastogi N. et al. Malont: An ontology for malware threat intelligence. *Deployable Machine Learning for Security Defense*. Cham: Springer International Publishing, 2020, pp. 28–44. DOI: 10.1007/978-3-030-59621-7_2
5. Kolesnikova D.S., Vereshchagina E.A., Gulyaev V.E. Designing the ontological model for the domain model of «Information Security». *Inzhenernyj vestnik Dona*, 2023, no. 7 (103), pp. 81–90. (In Russ.)
6. Piplai A. et al. Creating cybersecurity knowledge graphs from malware after action reports. *IEEE Access*, 2020, vol. 8, pp. 211691–211703. DOI: 10.1109/ACCESS.2020.3039234
7. Zhao X. et al. A survey on cybersecurity knowledge graph construction. *Computers and Security*, 2024, vol. 136, pp. 103524. DOI: 10.1016/j.cose.2023.103524
8. Kasimova A.R., Safiullina L.H. Use of digital twins in building the security system of the enterprise. *Mezhdunarodnyj forum Kazan Digital Week-2022: sbornik materialov Mezhdunarodnogo foruma*. Kazan': Nauchnyy tsentr bezopasnosti zhiznedeyatel'nosti, 2022, pp. 291–298. (In Russ.)
9. Smagin A.A., Poletaev V.S. A software tool for information security threats forecasting. *Infokommunikacionnye tehnologii*, 2018, vol. 16, no. 2, pp. 192–198. DOI: 10.18469/ikt.2018.16.2.06 (In Russ.)
10. Grebeshkov A.Y. Design of subject-oriented ontology for IEEE 802.22 cognitive access networks. *Infokommunikacionnye tehnologii*, 2018, vol. 16, no. 4, pp. 379–387. DOI: 10.18469/ikt.2018.16.4.03 (In Russ.)
11. Karpova N.E. et al. Development of the analyzing system for user's actions in the informational environment. *Dinamika sistem, mekhanizmov i mashin*, 2020, vol. 8, no. 2, pp. 114–123. (In Russ.)
12. ATT&CK Matrix for enterprise. URL: https://attack.mitre.org/ (accessed: 10.02.2025).

Received 18.02.2025
Accepted 18.03.2025