УДК 004.056.53

И.В. Котенко, О.В. Полубелова, А.А. Чечулин

ПОСТРОЕНИЕ МОДЕЛИ ДАННЫХ ДЛЯ СИСТЕМЫ МОДЕЛИРОВАНИЯ СЕТЕВЫХ АТАК НА ОСНОВЕ ОНТОЛОГИЧЕСКОГО ПОДХОДА

Котенко И.В., Полубелова О.В., Чечулин А.А. **Построение модели данных для системы моделирования сетевых атак на основе онтологического подхода.**
Аннотация. В статье рассматривается задача построения модели данных на основе онтологического подхода для системы моделирования сетевых атак, являющейся частью SIEM-системы. Приводится общая схема данных для данной системы, построенная на базе SCAP-протокола. Выполнен анализ релевантных работ, в которых рассматриваются использование онтологий для различных систем защиты информации. Более подробно в работе рассматривается построение онтологий для SCAP-протокола. В качестве примера реализации модели данных для системы моделирования сетевых атак предлагается онтология для представления модели уязвимостей.
Ключевые слова: сетевая безопасность: онтологии, уязвимости, модель данных.

Kotenko I.V., Polubelova O.V., Chechulin A.A. **Design of the ontology based data model for the network attack modeling system.**
Abstract. The paper considers the task of designing the ontology based data model for a network attack modeling system which is a part of a SIEM system. The common data scheme is suggested. The scheme was developed based on the SCAP protocol. Related papers on ontology based security systems are analyzed. The design of the SCAP protocol ontology is considered in more detail. The vulnerability ontology is proposed as an example of the common data model of the network attack modeling system.

Keywords: network security, ontology, vulnerability, data model.

1. Введение. В настоящее время одним из наиболее важных направлений исследований в области информационной безопасности компьютерных инфраструктур является технология управления информацией и событиями безопасности (Security Information and Event Management, SIEM). Значимым элементом, выполняющим роль организации межкомпонентного взаимодействия в SIEM-системах, является репозиторий. Существенным фактором, влияющим на эффективность работы различных компонентов SIEM-системы, является эффективность подхода к построению, изменению модели данных, а также к организации доступа к хранилищу.

В данной работе рассматривается онтологический подход для построения модели данных системы моделирования сетевых атак (СМСА), которая является одним из аналитических компонентов SIEM-системы.

Ранее авторы уже публиковали ряд работ, рассматривающих онтологический подход для построения репозитория в SIEM-системах [1–5]. Данная работа посвящена практическому аспекту разработки онтологической модели данных для одного из компонентов – системы моделирования сетевых атак.

СМСА осуществляет проактивный анализ событий и инцидентов, позволяющий расширить возможности и повысить точность выявления инцидентов, связанных с информационной безопасностью [6–8].

В качестве основы модели данных используется SCAP-протокол [6], включающий в себя стандарты представления событий, уязвимостей, метрик безопасности и др. СМСА в процессе своей работы загружает базу уязвимостей для проведения анализа защищенности компьютерной сети.

В статье демонстрируется пример реализации онтологии для представления уязвимости. Хранилище триплетов реализовано с использованием Virtuoso Server компании OpenLink [9]. При загрузке осуществляется трансляция в формат разработанной онтологии.

Статья организована следующим образом. В первом разделе приведен краткий анализ релевантной литературы. Во втором разделе рассматривается онтологический подход для построения модели данных SCAP-протокола. Третий раздел посвящен анализу входных и выходных данных СМСА, их связям с протоколом SCAP. В четвертом разделе приводится пример разработанной онтологии уязвимостей.

2. Анализ релевантных работ. При проведении анализа основных тенденций использования онтологий в системах защиты информации был выделен ряд работ.

В [10] рассматриваются корпоративные семантические веб-технологии. Авторы считают, что главная проблема широкого использования семантического подхода заключается в отсутствии онтологии шаблонов для событий, процессов, состояний, действий и других понятий, связанных с ее изменением с течением времени. Вместо этого нынешние семантические подходы пытаются построить общую супер-онтологию событий, но она игнорирует функционально важные различия в семантике приложений предметной области и в моделях событий, лежащих в их основе. Исходя из этого, авторы предлагают для описания событий использовать модульную и многоуровневую модель событий.

Таким образом, предполагается построить онтологию в виде иерархической структуры. Общие онтологии верхнего уровня будут охватывать основные концепции: время, события и т.д. Онтология

конкретной предметной области, приложения и задачи, выражающая общую модульную субонтологию онтологии верхнего уровня, формулирует более конкретные специализированные понятия. Для классов онтологии предметной области определяются конкретные события. Они могут иметь отношения с классами онтологий других предметных областей и могут иметь типы данных и свойства объекта. Онтологии конкретных предметных областей, приложений и задач, которые являются модульными субонтологиями общей онтологии верхнего уровня, задают более конкретные специализированные понятия. Определенные предметной областью события моделируются как классы онтологии предметной области и находятся в отношениях с классами онтологий других предметных областей. Они могут иметь свойства типов данных или объекта. Эта идея аналогична объектно-ориентированному подходу к разработке программного обеспечения.

В [11–12] рассматривается применение онтологического подхода для построения модели инцидента и предупреждения об угрозе. В качестве стандарта при построении модели используется SCAP-протокол.

Авторы [13] разработали онтологию для управления уязвимостями, которая может быть использована для представления, классификации, уменьшения влияния и администрирования уязвимостями, представленными в базе NVD.

Статья [14] посвящена проекту, выполняемому в компании MITRE, по построению общей онтологии для SCAP-протокола. В настоящий момент эта работа еще не завершена.

В [15] предлагается система для анализа уязвимостей на основе онтологического подхода. Здесь подробно рассмотрены различные модели представления уязвимостей в других исследовательских работах, в том числе и наличие ссылок на одинаковые уязвимости в различных общеизвестных базах уязвимостей.

В [16] рассматривается онтологический подход для представления активов, угроз, уязвимостей, контрмер и взаимосвязей между ними. Работа [17] заостряет внимание на построении онтологической модели для одной из базовых сущностей компонентов SIEM-системы - понятия события.

Анализ работ показывает, что направление применения онтологического подхода для систем защиты информации активно развивается. К его преимуществам в использовании для SIEM-систем можно отнести возможность построения модели данных в наиболее общем и в то же время не перегруженном виде, который должен быть

адаптирован для каждой области применения в процессе развертывания. Это свойство особенно значимо для SIEM-систем, которые развертываются в самых различных областях применения (критические инфраструктуры, сетевые инфраструктуры и т.д.)

Использование онтологий позволяет создавать общую модель, которая дополняется всеми необходимыми концептами в процессах интеллектуальных сервисов для различных предметных областей. Эффективность поисковых систем, основанных на онтологиях, позволяет аналитическим модулям уменьшить время, необходимое для извлечения из репозитория информации для анализа, и повысить качество результата поиска.

Онтологический подход к построению модели данных в интеллектуальных сервисах задает слабосвязанное, модульное представление, которое устойчиво к быстрым изменениям и сложности [14].

Вышеизложенные характеристики обосновывают его применение для построения систем защиты информации.

На основании рассмотренных работ в статье предлагается применение онтологического подхода для построения модели данных СМСА на примере онтологии уязвимостей.

При выборе основы для построения модели данных рассматривались различные стандарты, формализующие сущности предметной области информационной безопасности. К ним относятся, например, стандарт CIM (Common Information Model) [18], стандарт IDMEF (Intrusion Detection Message Exchange Format) [19] и ряд других.

Для реализации модели уязвимостей выбран стандарт протокола SCAP [21], включающий, в том числе, стандарт “Общие уязвимости и воздействий” (Common Vulnerabilities and Exposures, CVE). Такой выбор обусловлен тем, что СМСА использует “Национальную базу данных уязвимостей” (National Vulnerability Database, NVD), основанную на этом стандарте. Кроме того, протокол SCAP развивается и поддерживается компанией MITRE совместно с Американским Национальным институтом стандартизации и технологий (National Institute of Standards and Technology, NIST), который занимает ведущие позиции в области стандартизации.

3. Онтологический подход для построения модели данных SCAP-протокола. SCAP является спецификацией, которая объединяет ряд стандартов для унифицированного управления данными по безопасности. SCAP позволяет составить список используемых в

системе платформ и приложений, задать особенности их конфигурации, неблагоприятно влияющих на защищенность, специфицировать список уязвимостей, оценить неблагоприятное влияние конфигураций и уязвимостей, выявить наиболее критичные уязвимости (обнаружить присутствие уязвимостей и присвоить им оценки критичности).

SCAP включает в себя следующие стандарты:

- «Общее перечисление платформ» (Common Platform Enumeration – CPE) используется для описания программно-аппаратного обеспечения;
- «Общее перечисление конфигураций» (Common Configuration Enumeration – CCE) используется для описания особенностей программно-аппаратной конфигурации, неблагоприятно влияющих на защищенность;
- «Общие уязвимости и дефекты» (Common Vulnerabilities and Exposures – CVE) используется для описания списка уязвимостей данных продуктов;
- «Система оценивания уязвимостей» (Common Vulnerabilities Scoring System, CVSS) используется для оценки неблагоприятного влияния конфигураций и уязвимостей, выявления наиболее критичных уязвимостей, на основе чего потом проводится исправление ошибок.

На основе описанных выше стандартов, как правило, разрабатываются реляционные модели данных при разработке программного обеспечения в области управления информацией и событиями безопасности, а в качестве хранилища используются реляционные СУБД.

Однако существуют определенные трудности по выражению всех необходимых отношений между сущностями предметной области. Модель получается перегруженной, и выборка данных занимает значительное время. Это обусловлено также недостаточной гибкостью и низкой выразительностью языка запросов SQL, используемого в реляционных СУБД.

Второй проблемой является необходимость обновления схемы данных в соответствии с требованиями активно меняющейся предметной области. Для реляционных СУБД эта задача на больших объемах данных требует больших затрат ресурсов.

Одним из альтернативных решений по представлению данных в системах обработки информации сложной структуры является онтологический подход. Используя средства дескрипционной логики, он позволяет значительно проще выразить сложные отношения между сущностями.

Суть этого подхода заключается в том, что вначале выделяется набор концептов (базовых понятий данной предметной области). Затем строятся связи между концептами, т.е. определяются отношения и взаимодействия базовых понятий.

В самом простом случае онтология описывает только иерархию концептов-отношений, связанных отношениями категоризации. Концепты и отношения могут формулироваться с использованием дескрипционной логики, где термины словаря являются именами унарных и бинарных предикатов (соответственно концепты и отношения).

Такие аксиомы используются для полноты выражения отношений между концептами и для того, чтобы ограничить их предполагаемую интерпретацию. Таким образом, онтология представляет собой базу знаний, описывающую факты, которые предполагаются всегда истинными в рамках определенного сообщества на основе общепринятого смысла используемого словаря.

Отображение стандартов, касающихся SCAP, в онтологическую архитектуру, которое предполагается использовать в CMCA, показано на рис. 1 [14].

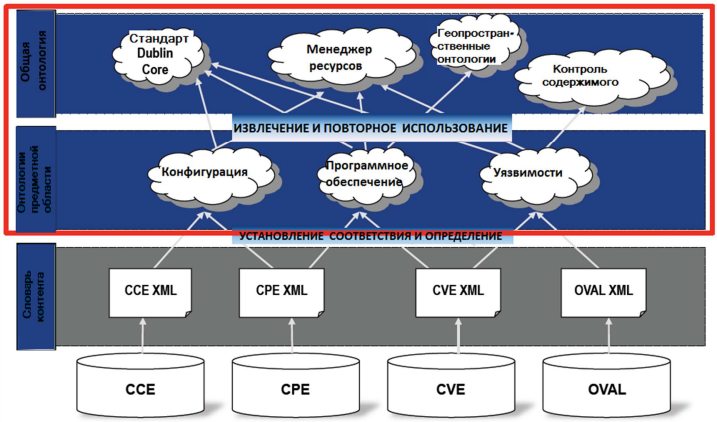

Рис. 1. Онтологическая архитектура для протокола SCAP.

Самый верхний слой онтологии на рис. 1 содержит общие онтологии. Они включают в себя стандартные онтологии метаданных “Дублинского ядра” (Dublin Core metadata standard ontology) [21], онтологию менеджера ресурсов, которая импортирует часть модели (Resource Manager) и ссылок “Дублинского ядра” SKOS (Simple Knowledge

Organization System) – простую систему организации знаний) [22], “контактную” онтологию (Point-of-Contact ontology), которая формируется на основе спецификации FOAF [23] и онтологии Vcard [24], а также онтологию контроля контента (Content Curation ontology).

4. Модель данных СМСА на базе SCAP-протокола. В данной работе рассматривается аспект построения модели данных для СМСА, поэтому опишем подробнее входные и выходные данные системы, представленные на рис. 2.

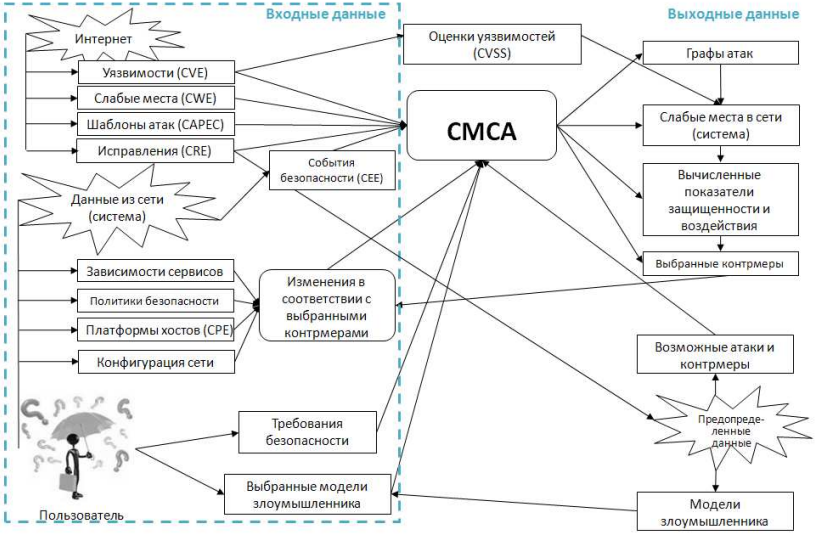

Рис. 2. Описание входных и выходных данных СМСА.

Часть входных данных (уязвимости, слабые места, шаблоны атак, а также исправления) СМСА загружаются из Интернета с помощью модуля обновления. При этом используется “Национальная база данных уязвимостей” (National Vulnerability Database, NVD) и “Открытая база данных уязвимостей” (Open Source Vulnerability DataBase, OSVDB). В процессе загрузки данные об уязвимостях и слабых местах транслируются во внутренние форматы, разработанные на основе CVE и CWE стандартов соответственно.

При построении модели данных использовался также стандарт CPE. На его основе описаны программно-аппаратные платформы, подверженные уязвимостям и слабым местам в стандартах CVE и CWE. Для формализации событий в общей схеме данных планируется ис-

пользовать стандарт CEE, но работа над ним еще не завершена. В процессе работы CMCA строит оценки уязвимостей на основе стандарта CVSS.

Для представления выходных данных CMCA в настоящий момент не используется стандартизация.

Большая часть описанных структур данных в CMCA реализована с применением реляционного подхода. Однако для повышения эффективности работы системы рассмотрим использование онтологии уязвимости.

5. Онтология уязвимостей (CVE) для CMCA. На рис. 3 представлена онтологическая модель, описывающая уязвимости программно-аппаратного обеспечения, производителей и другие понятия.

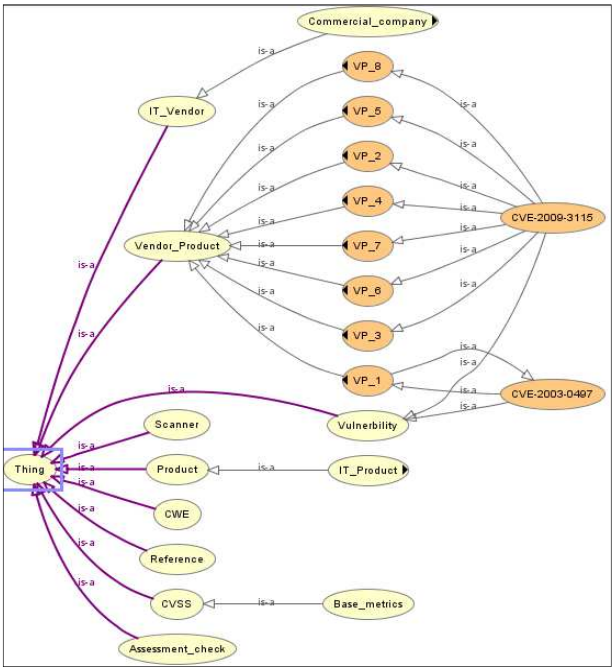

Рис. 3. Онтология уязвимостей.

Онтологическая модель, приведенная на данном рисунке, описывает иерархию и связи между концептами. Разработанная

онтология состоит из схемы данных, которая называется TBox (Terminology box), и самих данных – ABox (Assertion box).

Описание уязвимости в протоколе CVE представляет собой некоторую последовательность программно-аппаратных компонентов, соединенных логическими операторами (AND, OR, NOT AND, NOT OR). В рассматриваемой онтологии такие связи выражаются набором аксиом, что позволяет перенести в модель данных логику взаимосвязей концептов.

Следует отметить, что в реляционной модели список продуктов, приводящих к возникновению уязвимости, хранится в виде строки, и при необходимости загружается весь список уязвимостей, который анализировался программно.

Применение онтологического подхода с лежащей в его основе дескрипционной логикой позволяет решить задачу представления таких данных гораздо эффективнее, значительно уменьшить объем выборки и, соответственно, ускорить работу СМСА.

6. Заключение. В статье рассматривается построение модели данных на основе онтологического подхода для системы моделирования сетевых атак, являющейся частью SIEM-системы.

Проведен анализ релевантных работ, в которых рассматриваются онтологии для различных систем защиты информации. Анализ работ показывает, что применения онтологического подхода в этом направлении активно развивается. К его преимуществам в использовании для SIEM-систем можно отнести возможность построения модели данных в наиболее общем, не перегруженном виде, который должен быть расширен для каждой области применения в процессе развертывания. Одним из существенных преимуществ онтологического подхода по сравнению с реляционным является низкая ресурсоемкость внесения изменений в метасхему.

На основании рассмотренных работ в статье предлагается применение онтологического подхода для построения модели данных СМСА на примере онтологии уязвимости.

При выборе основы для построения модели данных рассматривались различные стандарты, формализующие сущности предметной области информационной безопасности. Для реализации модели уязвимостей был выбран стандарт протокола SCAP, включающий стандарт CVE.

В статье более подробно рассматривается построение онтологий для SCAP-протокола, предлагаемого компанией MITRE.

Приводится общая схема данных для CMCA, построенная на базе SCAP-протокола. В качестве примера реализации онтологии, предлагается онтология для представления модели уязвимостей.

Дальнейшие исследования связываются с расширением предложенной онтологии уязвимостей, реализацией остальных стандартов протокола SCAP с применением онтологического подхода. Планируется расширить разрабатываемую онтологическую модель для обеспечения возможности представления вырабатываемых контрмер, результатов оценки риска, модели нарушителя и других концептов, основываясь на протоколе SCAP.

Литература

1. *Котенко И.В., Полубелова О.В., Саенко И.Б., Чечулин А.А.* Применение онтологий и логического вывода для управления информацией и событиями безопасности // Системы высокой доступности . 2012. Т. 8. № 2 . С. 100-108.
2. *Котенко И.В., Саенко И.Б.* Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН . 2012. № 3 . С. 84-100.
3. *Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А.* Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН . 2012. № 1 . С. 27-56.
4. *Котенко И.В., Саенко И.Б.* Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах // Труды СПИИРАН . 2013. № 1 . С. 21-40.
5. *Котенко И.В., Юсупов Р.М.* Перспективные направления исследований в области компьютерной безопасности // Защита информации. Инсайд, № 2, 2006. С.46–57.
6. *Котенко И.В., Дойникова Е.В.* Анализ протокола автоматизации управления данными безопасности SCAP // Защита информации. Инсайд, 2012, № 2, С.56-63.
7. *Kotenko I., Chechulin A.* Attack Modeling and Security Evaluation in SIEM Systems // International Transactions on Systems Science and Applications, Vol.8, December 2012. P.129-147.
8. *Kotenko I., Chechulin A., Novikova E.* Attack Modelling and Security Evaluation for Security Information and Event Management // SECRYPT 2012. International Conference on Security and Cryptography. Proceedings. Rome, Italy. 24–27 July 2012. P. 391-394.
9. Virtuoso Universal Server. OpenLink Software. http://virtuoso.openlinksw.com
10. *Teymourian K., Paschke A.* Towards Semantic Event Processing // Proceedings of the Third ACM International Conference on Distributed Event-Based Systems (DEBS '09). ACM. New York, 2009. P. 347-352.
11. *Lopez de Vergara, Jorge E.; Villagra, Victor A.; Holgado, Pilar; et al.* A semantic web approach to share alerts among Security Information Management Systems // Web Application Security V.72.2010. P.27-38
12. *López de Vergara J. E., Villagrá V. A., Berrocal J.* Applying the Web Ontology Language to management information definitions // IEEE Communications Magazine, 2004. P. 68-74.

13. *Guo M., Wang J. A.* An Ontology-based Approach to Model Common Vulnerabilities and Exposures in Information Security // Proceedings of the 2009 ASEE SE Section Conference, 2009. 10 p.
14. *Parmelee M. C.* Toward an Ontology Architecture for Cyber-Security Standards // Proceedings of the 2010 Semantic technology for intelligence, defense, and security conference, 2010. 8 p.
15. *Elahi G., Yu E., Zannone N. A* Modeling Ontology for Integrating Vulnerabilities into Security Requirements Conceptual Foundations // Proceedings of the 28th International Conference on Conceptual Modeling, 2009. P. 99-114.
16. *Herzog A., Shahmehri N., Duma C.* An ontology of information security // International Journal of Information Security and Privacy. V. 1(4). 2007. P.1-23.
17. *Schütte J., Rieke R., Winkelvos T.* Model-Based Security Event Management // Proceedings of the 6th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security. 2012. P.181-190.
18. CIM, Common Information Model – Distributed Management Task Force, Inc. – http://dmtf.org/standards/cim
19. Intrusion Detection Exchange Format. http://xml.coverpages.org/idmef.html
20. Протокол SCAP. http://www.nist.gov/index.html.
21. Dublin Core Metadata Element Set, Version 1.1 Dublin Core Metadata Initiative. http://dublincore.org/documents/dces/
22. *Miles A., Bechhofer S.* SKOS Simple Knowledge Organization System. Reference. W3C Recommendation. 18 August 2009. http://www.w3.org/TR/skos-reference/
23. *Brickley D., Miller L.* FOAF Vocabulary Specification. Namespace Document. 9 August 2010. http://xmlns.com/foaf/spec/
24. *Brickley D., Miller L.* W3C: Representing vCard Objects in RDF. W3C Member Submission. 20 January 2010. http://www.w3.org/Submission/vcard-rdf/

Котенко Игорь Витальевич — д-р техн. наук, проф., заведующий лабораторией проблем компьютерной безопасности, СПИИРАН. Область научных интересов: безопасность компьютерных сетей, в том числе управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома и управление цифровыми правами, технологии моделирования и визуализации для противодействия кибер-терроризму. Число научных публикаций — более 450. ivkote@comsec.spb.ru, www.comsec.spb.ru; СПИИРАН, 14-я линия В.О., д.39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328–2642, факс +7(812)328–4450.

Kotenko Igor Vitalievich — Ph.D., Professor, Head of Laboratory of Computer Security Problems, SPIIRAS. Research interests: computer network security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems, digital right management, modeling, simulation and visualization technologies for counteraction to cyber terrorism; The number of publications — more 450. ivkote@comsec.spb.ru, www.comsec.spb.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812) 328–2642, fax +7(812)328–4450.

Полубелова Ольга Витальевна — научный сотрудник лаборатории проблем компьютерной безопасности, СПИИРАН. Область научных интересов: Безопасность компьютерных сетей, включая управление политиками безопасности, верификация

протоколов безопасности и систем безопасности, использование методов проверки на модели для обнаружения и разрешения конфликтов в политиках; онтологии в информационной безопасности, дескрипционные логики, СИЕМ-системы. Число научных публикаций — 25. ovp@comsec.spb.ru, www.comsec.spb.ru; СПИИРАН, 14-я линия В.О., д.39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-2642, факс +7(812)328-4450. Научный руководитель — Котенко И.В.

Polubelova Olga Vitalievna — researcher of Laboratory of Computer Security Problems, SPIIRAS. Research interests: computer network security, including policy management, verification of security protocols and security systems, model checking techniques for policy conflicts detection and resolution, ontology, description logic, SIEM systems. The number of publications — 25. ovp@comsec.spb.ru, www.comsec.spb.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812) 328-2642, fax +7(812)328-4450. Scientific adviser — I.V. Kotenko.

Чечулин Андрей Алексеевич —научный сотрудник лаборатории проблем компьютерной безопасности, СПИИРАН. Область научных интересов: безопасность компьютерных сетей, обнаружение вторжений, анализ сетевого трафика, анализ уязвимостей. Число научных публикаций — 70. chechulin@comsec.spb.ru; СПИИРАН, 14-я линия В.О., 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328–2642, факс +7(812)328–4450. Научный руководитель — И.В. Котенко.

Chechulin Andrey Alexeevich —research scientist of Laboratory of Computer Security Problems, SPIIRAS. Research interests: computer network security, intrusion detection, analysis of the network traffic, analysis of vulnerability. The number of publications — 70. chechulin@comsec.spb.ru; SPIIRAS, 14-th line, 39, St. Petersburg, 199178, Russia; office phone +7(812) 328–2642, fax +7(812)328–4450. Supervisor — I.V. Kotenko.

Поддержка исследований. В публикации представлены результаты исследований, поддержанные Министерством образования и науки Российской Федерации (государственный контракт 11.519.11.4008), грантами РФФИ (проект 13-01-00843-а), программой фундаментальных исследований ОНИТ РАН (№ 2.2) и проектами Седьмой рамочной программы Европейского Союза *SecFutur* и *MASSIF*.

Рекомендовано лабораторией проблем компьютерной безопасности СПИИРАН.
Заведующий лабораторией Котенко И.В., д-р техн. наук, проф.
Статья поступила в редакцию 04.03.2013.

РЕФЕРАТ

Котенко И.В., Полубелова О.В., Чечулин А.А. **Построение модели данных для системы моделирования сетевых атак на основе онтологического подхода.**

В настоящее время одним из наиболее важных направлений исследований в области информационной безопасности компьютерных инфраструктур является технология управления информацией и событиями безопасности (Security Information and Event Management, SIEM). Значимым элементом, выполняющим в SIEM-системах роль организации межкомпонентного взаимодействия, является репозиторий.

Существенным фактором, влияющим на эффективность работы различных компонентов SIEM-систем, является выбранный подход к построению и изменению модели данных, а также к организации доступа к хранилищу.

В статье рассматривается задача построения модели данных на основе онтологического подхода для системы моделирования сетевых атак, являющейся частью SIEM-системы. Приводится общая схема данных для данной системы, построенная на базе SCAP-протокола. Выполнен анализ релевантных работ, в которых рассматриваются использование онтологий для различных систем защиты информации. Более подробно в работе рассматривается построение онтологий для SCAP-протокола. В качестве примера реализации модели данных для системы моделирования сетевых атак, предлагается онтология для представления модели уязвимостей.

SUMMARY

Kotenko I.V., Polubelova O.V., Chechulin A.A. **Design of the ontology based data model for the network attack modeling system.**

The technology of Security Information and Event Management (SIEM) is now one of the most important research directions in the field of information security of computer infrastructures. Repository is an important element that participates in the interaction of components of SIEM systems.

Important factor affecting the performance of various components of SIEM systems is the approach to data model construction and alteration, as well as to the organization of access to the repository.

The paper considers the task of designing the ontology based data model for a network attack modeling system which is a part of a SIEM system. The common data scheme is suggested. The scheme was developed based on the SCAP protocol. Related papers on ontology based security systems are analyzed. The design of the SCAP protocol ontology is considered in more detail. The vulnerability ontology is proposed as an example of the common data model of the network attack modeling system.