2. Аграновский А. В. и др. Основы компьютерной стеганографии: учебное пособие для вузов. Москва: Радио и связь. 2003. 152 с.
3. Быков С. Ф. Алгоритм сжатия JPEG с позиции компьютерной стеганографии // Защита информации. Конфидент. 2000. №3. С. 26–33.
4. Миано Дж. Форматы и алгоритмы сжатия изображений в действии: учебное пособие. Москва: Триумф. 2003. 336 с.
5. Tinsley R. Steganography and JPEG Compression: Final Year Project Report. University of Warwick, UK, 1996. 114p.
6. Цветовая субдискретизация понятным языком – немного отдаем, чтобы много выиграть [Электронный ресурс]. – Режим доступа: http://projectorworld.ru/blog/957.html. – Дата доступа: 11.12.2019.
7. Пиковое отношение сигнала к шуму [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/?oldid=102495551. – Дата доступа: 02.10.2019.
8. Чваркова И. Л. Повышение пропускной способности и стойкости стеганографических систем: диссертация на соискание степени кандидата технических наук // Минск. 2008.

СТРУКТУРА МЕТОДИКИ МОДЕЛИРОВАНИЯ УГРОЗ КОМПЬЮТЕРНЫХ СИСТЕМ НА ОСНОВЕ ПРЕДМЕТНО-ОРИЕНТИРОВАННЫХ МОДЕЛЕЙ

А. И. Бражук

ГрГУ им. Я. Купалы, г. Гродно, Республика Беларусь
E-mail: brazhuk@grsu.by

Предложена методика моделирования угроз компьютерных систем на основе предметно-ориентированных моделей угроз, которая позволяет автоматически формировать списки релевантных угроз и контрмер на основе описаний архитектур компьютерных систем (диаграмм потоков данных). Методика использует язык онтологий OWL и функции автоматического логического вывода. В отличие от существующих решений методика позволяет внедрить объектно-ориентированный подход, обеспечить интеграцию с источниками связанных открытых данных и представлять контрмеры как контекстные шаблоны безопасности.

Ключевые слова: моделирование угроз; онтология; OWL.

Введение. Моделирование угроз компьютерных систем с использованием диаграмм потоков данных (DFD - Data Flow Diagram) было предложено некоммерческой организацией OWASP (Open Web Application Security Project) и корпорацией Microsoft. Для декомпозиции структуры приложения и описания потоков данных, команда разработчиков применяет простое визуальное представление архитектуры приложения посредством диаграмм DFD; на последующих стадиях полученные диаграммы используются для построения неформальной модели угроз (перечня угроз и противодействий этим угрозам) путем дискуссий с приме-

нением сведений из существующих каталогов угроз, уязвимостей, атак и т. д. Основные проблемы в данной области связаны с отсутствием как формальных подходов для описания архитектур компьютерных систем, так и хорошо структурированных источников знаний об угрозах и контрмерах.

Предметно-ориентированные модели угроз. Для детализации и расширения существующих риск-ориентированных моделей при решении задач моделирования угроз нами предложено использовать предметно-ориентированные модели угроз [1], которые направлены на решение ряда практических задач, таких как детализация контрмер, сравнение эффективности различных средств защиты, автоматизация моделирования угроз.

Источниками знаний о проблемах безопасности некоторой предметной области (облачные технологии, интернет вещей или программно-определяемые сети) являются: перечисления и каталоги угроз, атак, уязвимостей; каталоги шаблонов безопасности; а также различные документы, описывающие опыт безопасного проектирования компьютерных систем (руководства, лучшие практики, шаблоны проектирования).

Результатом анализа существующих источников является база знаний, или формализованная предметно-ориентированная (мета) модель угроз, представляющая собой совокупность трех подмоделей:

- *подмодель архитектурных компонентов*, т. е. иерархический список всех элементов (компоненты, потоки данных, границы), которые может иметь компьютерная система данного типа;
- *подмодель угроз*, т. е. иерархический список возможных угроз для данной предметной области, с контекстными определениями и определенными зависимостями с потоками данных и противодействиями;
- *подмодель противодействий* (контекстных шаблонов безопасности), т. е. иерархический список контекстных шаблонов безопасности, специфичных для данной предметной области, с контекстными определениями и зависимостями от потоков данных и угроз.

Данная база знаний должна быть снабжена механизмами, позволяющими устанавливать сложные зависимости между архитектурными компонентами, угрозами и контрмерами, а также ранжировать угрозы и противодействия в соответствие с целями анализа. Простейшей моделью целей безопасности является триада CIA (C — Confidentiality, I — Integrity, A — Availability. Также предлагается дополнительно использовать аутентификацию (Authentication), неотказуемость (Non-Repudiation) и авторизацию (Authorization). Альтернативным вариантом меток является модель STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) для классификации угроз.

Для реализации предметно-ориентированных моделей угроз предлагается использовать онтологии OWL (Web Ontology Language) и данные из различных семантических источников знаний, как специализированных, так и общего назначения, например, Wikidata и DBpedia.

Структура методики. Предложенная нами методика позволяет, используя соответствующую предметно-ориентированную модель угроз, автоматически сформировать список релевантных угроз и противодействий угрозам (контрмер) на основе описания архитектуры компьютерной системы, представленной в виде DFD диаграммы.

Методика включает алгоритмы построения предметно-ориентированных моделей угроз и соответствующих библиотек компонентов диаграмм потоков данных, а также алгоритм формирования списков угроз и противодействий.

Методика основана на *базовой онтологической модели угроз* [2]. Базовая модель обеспечивает семантическую интерпретацию описаний архитектур компьютерных систем и автоматическое формирование моделей угроз; реализована на языке OWL.

Моделирование угроз для некоторого типа (домена) компьютерных систем обеспечивается двумя типами моделей (рис. 1):

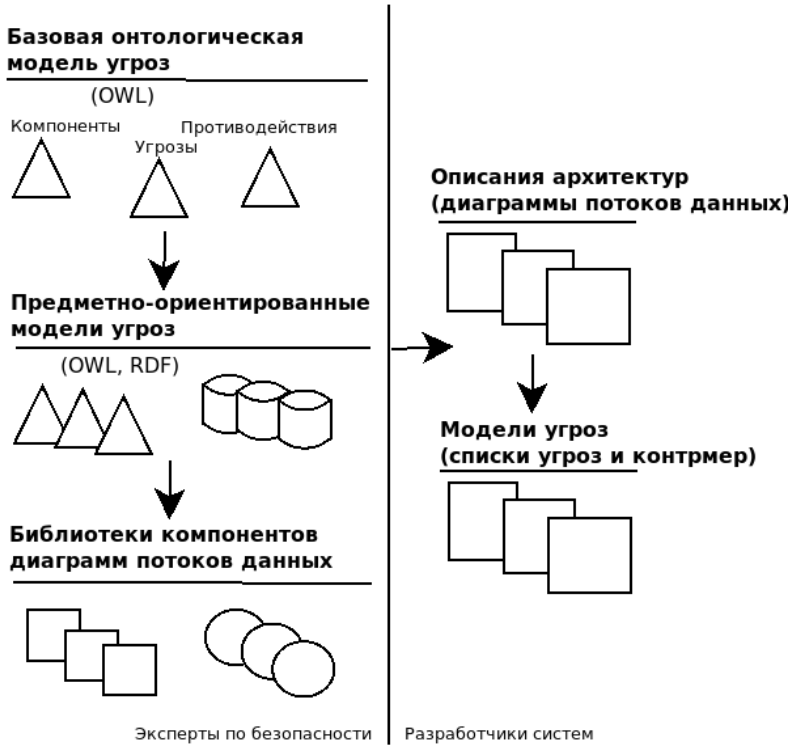

Рис. 1. Структура методики моделирования угроз

- *Предметно-ориентированная модель угроз*. Чтобы построить предметно-ориентированную модель угроз, эксперты по безопасности долж-

ны расширить базовую модель угроз, добавив определенные компоненты, угрозы и противодействия, относящиеся к данному домену.

- *Предметно-ориентированная библиотека компонентов DFD*. Содержит перечень компонентов диаграмм DFD, которые могут использоваться для создания диаграмм, представляющих структуры систем из данной предметной области. Для создания библиотек используются соответствующие программные процедуры.

Моделирование угроз определенной компьютерной системы можно представить последовательностью трех шагов:

- *Представление архитектуры системы как DFD диаграммы*. Системный архитектор представляет структуру своей системы как диаграмму (или как набор диаграмм), используя элементы из соответствующей библиотеки компонентов DFD.

- *Семантическая интерпретация DFD диаграммы*. Соответствующие программные процедуры автоматически интерпретируют диаграмму как набор семантических сущностей (компоненты, потоки данных, границы и отношения между ними) и комбинируют этот набор с соответствующей предметно-ориентированной моделью угроз.

- *Автоматический логический вывод релевантных угроз и противодействий*. Процедуры автоматического логического вывода находят релевантные угрозы и противодействия из семантической интерпретации и предметно-ориентированной модели угроз. Затем программные процедуры способны построить списки угроз и противодействий для системы.

Реализация методики. В настоящее время реализована базовая онтологическая модель как онтология OWL; также для тестирования и апробации разрабатываемых программных средств разработана общая онтологическая модель угроз облачных вычислений. Соответствующие файлы OWL опубликованы в открытом доступе посредством сервиса GitHub (https://github.com/nets4geeks/OdTM). Для реализации модели был использован редактор онтологий Protege (http://protege.stanford.edu/).

Заключение. В данной работе предложена методика моделирования угроз компьютерных систем, которая позволяет, используя соответствующие предметно-ориентированные модели, автоматически формировать списки релевантных угроз и контрмер на основе описаний архитектур компьютерных систем. Методика основана на онтологическом подходе и использует язык онтологий OWL и функции автоматического логического вывода.

В отличие от существующих решений (неформальный подход, графовые модели, низкоуровневое логическое программирование [3, 4, 5]), методика позволяет внедрить объектно-ориентированный подход к моделированию угроз и обеспечить интеграцию разрабатываемых моделей

с источниками связанных открытых данных; ранжировать угрозы и контрмеры в соответствие с универсальными метками безопасности; а также представлять контрмеры как контекстные шаблоны безопасности.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. Олизарович Е. В., Бражук А. И. Концептуальные основы анализа моделей информационной безопасности облачных систем класса «Инфраструктура как услуга» // Доклады БГУИР. 2019. №. 6. С. 12–19.
2. Brazhuk A., Olizarovich E. Framework for ontology-driven threat modelling of modern computer systems // International Journal of Open Information Technologies. 2020. Vol. 8, №. 2. P. 14–20.
3. Sion L. et al. Solution-aware data flow diagrams for security threat modeling // SAC'18: Proceedings of the 33rd Annual ACM Symposium on Applied Computing. 2018. P. 1425–1432. DOI: 10.1145/3167132.3167285
4. Berger B.J., Sohr K., Koschke R. Automatically extracting threats from extended data flow diagrams // ESSoS 2016: Proceedings of the 8th International Symposium on Engineering Secure Software and Systems. 2016. P. 56–71. DOI: 10.1007/978-3-319-30806-7_4
5. Saatkamp K. et al. An Approach to Determine and Apply Solutions to Solve Detected Problems in Restructured Deployment Models using First-order Logic // Proceedings of the 9th International Conference on Cloud Computing and Services Science. 2019. Vol. 1. P. 495–506. DOI: 10.5220/0007763204950506

НАЗЕМНАЯ СТАНЦИЯ ПРИЕМА ТЕЛЕМЕТРИИ И ОПРЕДЕЛЕНИЯ ОРБИТЫ СВЕРХМАЛОГО КОСМИЧЕСКОГО АППАРАТА

А. П. Верстаковская, В. Е Евчик, А. Г. Кезик, В. А. Саечников, С. А. Соловьев, А. А. Спиридонов, Д. В. Ушаков, В. Е. Черный

Белорусский государственный университет, Минск, Беларусь
E-mail: sansan@tut.by

Задачи надежного приема телеметрии и определения орбитальных параметров являются актуальными для сверхмалых космических аппаратов. Описаны программно-аппаратные средства построения наземной станции приема телеметрии сверхмалых космических аппаратов с возможностью определения параметров орбиты. Рассмотренная наземная станция приема позволит расширить географии приема, улучшить качество принимаемой информации, работать в автономном режиме, измерять орбитальные параметры, на практике обучать студентов технологиям приема телеметрии и определения орбит космических аппаратов.

Ключевые слова: наземная станция; сверхмалые космические аппараты; телеметрия; определение орбиты.