УДК 004.934.2

Вестник УрФО № 3(29) / 2018, с. 18–22

Гаршина В. В., Степанцов В. А.

DOI: 10.14529/SECUR180303

ОНТОЛОГИЧЕСКИЙ ПОДХОД ДЛЯ АНАЛИЗА РИСКОВ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

В статье предлагается метод формирования комплекса мер по обеспечению безопасности корпоративных информационных систем на основе анализа рисков, проводимого с использованием онтологического подхода. Приводится анализ применения методов оценки уровня угроз в зависимости от анализируемой информации: источников, вида представления, объективности и надежности.

Ключевые слова: *онтология, анализ рисков, информационная безопасность, модель идентификации угроз STRIDE.*

Garshina V. V., Stepantsov V. A.

ONTOLOGICAL APPROACH FOR RISK ANALYSIS SECURITY OF INFORMATION SYSTEMS

The article proposes a method of forming a set of measures to ensure the security of corporate information systems based on a risk analysis carried out using an ontological approach. The analysis of the application of methods for assessing the level of risk is presented depending on the information analyzed: sources, type of representation, objectivity and reliability.

Keywords: *ontology, risk analysis, information security, STRIDE threat identification model.*

Одним из перспективных направлений в области формализации знаний и их эффективной компьютерной обработки, являются онтологии. Они представляют описание структурной спецификации предметной области, включающее словарь терминов этой области (концептов, понятий, классов), набор отношений между понятиями которые описывают, как эти термины соотносятся между собой и наборы функций интерпретации (аксиоматизация), на понятиях и/или отношениях [1].

Формально онтология определяется как

$$O = \langle X, R, F \rangle$$

где X – конечное непустое множество терминов (концептов, понятий, классов) предметной области, R – конечный набор отношений между понятиями; F – конечное множе-

ство функций интерпретации (аксиоматизация), на понятиях и/или отношениях.

Онтологии классифицируются по типам в зависимости от конкретной задачи:

Мета-онтологии (Top-level ontologies) – описывают наиболее общие понятия, которые не зависят от предметных областей.

Онтология предметной области (Domain-ontologies) – формальное описание предметной области, применяется для уточнения понятий, определённых в мета-онтологии и определяет общую терминологическую базу предметной области.

Онтология конкретной задачи (Task ontologies) – онтология, определяющая общую терминологическую базу, относящуюся к конкретной задаче.

Сетевые онтологии (Application ontologies) – часто используются для описания конечных результатов действий, выполняемых объектами предметной области или задачи.

В случае если набор *R* и множество *F* являются пустыми, то такая онтология представляет собой глоссарий. Если *R* состоит из единственного отношения типа «подкласс-класс», а *F* – пусто, то онтология представляет собой таксономию.

Рассмотрим возможность применения онтологического подхода для анализа рисков безопасности информационных систем. Для этого необходимо определить методологическую основу для проведения анализа рисков и разработать соответствующую онтологию, объединяющую онтологию предметной области и онтологию решения задачи определения методов и выбору технологий защиты.

Комплекс мер по обеспечению безопасности корпоративных информационных систем формируются на основе анализа рисков. Реальные риски являются интегральной оценкой способности имеющихся в наличии средств защиты эффективно противодействовать угрозам информационной безопасности. На практике принято использовать следующие группы методов оценки рисков безопасности:

1. Группа методов определяющих уровень риска с помощью оценки степени соответствия определенному набору требований по обеспечению информационной безопасности. Основаны на нормативно-правовых материалах организации; требованиях действующего законодательства РФ, руководящие документы ФСТЭК, СТР-К, требования ФСБ РФ, ГОСТы; рекомендации международных стандартов – ISO 17799, OCTAVE, CoBIT; рекомендации компаний-производителей программного и аппаратного обеспечения.

2. Методы оценки рисков информационной безопасности основываются на определении вероятности реализации атак, а также уровней их ущерба. Количественный показатель риска вычисляется отдельно для каждой атаки и в общем случае является произведением вероятности проведения атаки на величину возможного ущерба от этой атаки. Материальный и моральный ущерб определяется собственником информационной системы, а вероятность атаки вычисляется группой экспертов на основе процедуры аудита.

При использовании данных методов применяются как количественные, так и качественные шкалы на основе которых определяются величины риска информационной безопасности. В случае применения количественных шкал, вероятность реализации атаки выражается числом в интервале [0,1], а ущерб определяется денежным эквивалентом материальных и моральных потерь, которые может понести организация в случае успешного проведения атаки. В случае применения качественных шкал используются нечеткие смысловые уровни, причем каждому такому уровню ставится в соответствие определенный интервал количественной шкалы оценки. В зависимости от применяемых методик оценки рисков число уровней может быть различным.

Важнейшими задачами защиты данных в информационных системах являются:

1) обеспечение строго санкционированного доступа к данным (availability), 2) обеспечение конфиденциальности данных (confidentiality),

3) обеспечение целостности данных (integrity).

Мероприятия по предотвращению или снижению критичности угроз информационной системе реализуются на следующих этапах:

1) классификация угроз безопасности;

2) определение методов защиты;

3) выбор технологии защиты.

Реализация первого этапа может быть выполнена в соответствии с подходом фирмы Microsoft на основе модели идентификации угроз STRIDE (**S**poofing identity, **T**ampering with data, **R**epudiation, **I**nformation disclosure, **D**enial of service, **E**levation of privilege) и мето-

дики DREAD (**D**amage potential, **R**eproducibility, **E**xploitability, **A**ffected users, **D**iscoverability) для оценки рисков угроз [2].

В соответствии с моделью STRIDE осуществляется классификация угроз:

Spoofing identity (подмена сетевых объектов) – атаки подобного типа позволяют взломщику выдавать себя за другого пользователя путем воспроизведения транзакции, выполняющей аутентификацию пользователя, а также осуществлять подделку электронных сообщений и пакетов аутентификации.

Tampering with data (фальсификация данных) – несанкционированное изменение данных с целью атаки, в частности модификация аутентификационных файлов с целью добавления нового пользователя, подделка электронных сообщений, модификация данных, передаваемых по сети.

Repudiation (отказ от ответственности) – отсутствие фиксации в системных журналах действий, которые могут привести к нарушению безопасности, контрагент отказывается от совершенного им действия (или бездействия), пользуясь тем, что у другой стороны нет никакого способа доказать обратное.

Information disclosure (раскрытие информации) – несанкционированный доступ к конфиденциальной информации, публикация конфиденциальной информации.

Denial of service (отказ в обслуживании) – атаками такого типа взломщик пытается лишить доступа к сервису правомочных пользователей путем заполнения сети пакетами SYN и излишней загрузкой сетевых ресурсов фальшивыми пакетами ICMP.

Elevation of privilege (повышение привилегий) – несанкционированное присваивание прав системного администратора, присваивание прав администратора используя переполнение буфера, в результате чего непривилегированный пользователь получает привилегированный доступ, позволяющий ему взломать или даже уничтожить систему.

Для выбора методов защиты на втором этапе необходимо выполнить количественную оценку риска опасности для конкретной информационной системы по методике DREAD:

Damage potential (потенциальный ущерб) – мера реального ущерба от успешной атаки. Наивысшая степень опасности равная 10 означает практически беспрепятственный взлом средств защиты и выполнение практически любых операций.

Reproducibility (воспроизводимость) – мера возможности реализации опасности. Некоторые бреши доступны постоянно, при этом оценка равна 10, другие – только в зависимости от ситуации, их доступность не предсказуема.

Exploitability (подверженность взлому) – мера усилий и квалификации, необходимых для атаки. В случае, если атаку может реализовать пользователь невысокой квалификации с домашнего компьютера – оценка опасности 10. Если же для ее проведения надо потратить 100 000 000 долларов, оценка опасности – 1. Атака, для которой можно написать алгоритм и распространить в виде сценария среди непрофессионалов, также оценивается в 10 баллов.

Affected users (группы пользователей, попадающих под удар) – доля пользователей, работа которых нарушается из-за успешной атаки. Оценка выполняется на основе процентной доли, если нарушается работа 100 % пользователей, то оценка 10, а 10 % – 1 балл.

Discoverability (возможность раскрытия атаки) – в силу того, что любая опасность поддается реализации, то практически всегда оценивается в 10 баллов.

Суммарное значение риска рассчитывается по следующей формуле

$$Risk - DREAD = (DMG + R + E + AU + D)/5$$

где DMG – Damage, R – Reproducibility, E – Exploitability, AU – Affected users и D – Discoverability.

Оценка рисков является главной целью в процессе управления информационными системами. Для минимизации уровня рисков требуется анализировать риски информационной безопасности и на основе этого анализа принимать эффективные решения по определению методов и выбору технологий защиты.

Разработка онтологии анализа рисков проводилась в специализированном онтологическом редакторе Protégé, предназначенном для создания онтологий различных предметных областей. Protégé позволяет проектировать онтологии, раскрывая иерархическую структуру классов и проводить тестирование правильности структуры и системы выводов по онтологии. Этот инструмент поддерживает язык OWL (Web Ontology Language), позволяет генерировать HTML-документы, которые отражают структуру онтологии. OWL онтология содержит описания классов, их характеристики и связи. Исполь-

зуя формальную семантику OWL и указанные данные, возможно получение информации, которая не была явно описана в онтологии, но следует из семантики данных [3].

При проектировании классов онтологии были разработаны: Абстрактный класс *Атака*, содержащий все классы предметной области и задачи анализа рисков, представляет собой верхний уровень онтологии. Набор требований безопасности к информационной системе содержится в классе *Требования безопасности*, его атрибутами являются атрибуты обеспечения строго санкционированного доступа (availability), обеспечения конфиденциальности (confidentiality) и целостности данных (integrity) со своими приоритетами. Набор подклассов модели идентификации атак STRIDE включается в класс *Типы атак*. Класс *Анализ риска* содержит набор подклассов методики DREAD.

На основе поступающих сведений о ситуации угрозы, в онтологии генерируется экземпляры классов, свойства классов получают значения и на основе структурных и семантических отношений, описанных в онтологии строиться логический вывод об уровне риска и, соответственно, выборе методов и технологий защиты.

Заключение о безопасности анализируемой системы строится на основе разработанных и размещенных в онтологии правил. Для задания собственных правил логических выводов используется стандарт SWRL. Каждое правило состоит из двух частей – условия и вывода, который формируется, если условие выполнено. И условие, и вывод могут состоять из нескольких атомов – элементарных логических выражений. Каждый атом представляет собой предикат – утверждение о каких-либо объектах онтологии. Правила SWRL позволяют создавать гибкие условия для получения новых знаний. На основе таких правил строится вывод о защищенности системы.

Механизмы логического вывода обеспечивают вычисление значений логических выражений, оценку правильности модели, позволяют автоматически помещать в онтологию новую информацию в соответствии с правилами, оперировать именами классов, свойств и сущностей, и «задавать модели вопросы», абстрагируя пользователя от подробностей внутреннего строения модели.

Стандарт языка SPARQL [4] описывает синтаксис запросов к онтологическим моделям (является аналогом языка SQL). Применяется преимущественно для выборки необходимых данных с помощью SELECT-запросов с возможной их фильтрацией и сортировкой. SPARQL поддерживает вопросы, требующие однозначных ответов да или нет, сортировку, фильтрацию, сопоставление строк.

В целях информационной безопасности всегда требуется анализировать риски и принимать эффективные решения по определению методов и выбору технологий защиты. Предлагаемый онтологический подход позволит эффективно использовать полученные знаний для решения задачи комплексного анализа рисков безопасности информационных систем.

Литература

1. Semantic Web / [Электронный ресурс]. – Режим доступа: https://elite.polito.it/teaching/past-courses/360-01rrdiu-semantic-web, свободный (дата обращения 09.06.2018).

2. Ховард М., Лебланк Д. Защищенный код: Пер. с англ, – 2-е изд., испр. М.: Издательско-торговый дом «Русская Редакция», 2004. – 704 с.

3. A. Herzog, N. Shahmehri, C. Duma, An Ontology of Information Security, International Journal of Information Security and Privacy, 1(4):1-23, 2007.

4. Стандарты W3C Консорциума / [Электронный ресурс]. – Режим доступа: https://www.w3.org/ , свободный (дата обращения 09.06.2018).

Refereces

1. Semantic Web / [EHlektronnyj recurs]. – Rezhim dostupa: https://elite.polito.it/teaching/past-courses/360-01rrdiu-semantic-web, svobodnyj (data obrashcheniya 09.06.2018).

2. K. Hovard M., Leblank D. Zashhishhennyj kod: Per. s angl, – 2-e izd., ispr. M.: Izdatel'sko-torgovyj dom «Russkaya Redaktsiya», 2004. – 704 s.

3. A. Herzog, N. Shahmehri, C. Duma, An Ontology of Information Security, International Journal of Information Security and Privacy, 1(4):1-23, 2007.

4. Стандарты W3C Консорциума / [EHlektronnyj recurs]. – Rezhim dostupa: https://www.w3.org/ , svobodnyj (data obrashcheniya 09.06.2018).

ГАРШИНА Вероника Викторовна, кандидат технических наук, доцент, доцент кафедры технологий обработки и защиты информации, федеральное государственное бюджетное образовательное учреждение высшего образования «Воронежский государственный университет», Россия, 394018, г. Воронеж, Университетская пл., 1. E-mail: garshina@cs.vsu.ru.

СТЕПАНЦОВ Вячеслав Алексеевич, кандидат технических наук, доцент, доцент кафедры технологий обработки и защиты информации, федеральное государственное бюджетное образовательное учреждение высшего образования «Воронежский государственный университет», Россия, 394018, г. Воронеж, Университетская пл., 1. E-mail: mrstep@yandex.ru

VERONIKA Garshina, Candidate of Engineering Science, Docent, Department of Processing Technology and Information Security in Voronezh State University. 1 Universitetskaya pl., Voronezh, 394018, Russia. E-mail: garshina@cs.vsu.ru

VYACHESLAV Stepantsov, Candidate of Engineering Science, Docent, Department of Processing Technology and Information Security in Voronezh State University. 1 Universitetskaya pl., Voronezh, 394018, Russia. E-mail: mrstep@yandex.ru