УДК 004.056 + 002:004.056 Вестник УрФО № 2(28) / 2018, с. 36–42

Кляус Т. К., Наумов А. Д., Гатчин Ю. А., Бондаренко И. Б.

СРАВНИТЕЛЬНОЕ ИССЛЕДОВАНИЕ ПРИМЕНИМОСТИ ДЕРЕВЬЕВ АТАК-КОНТРМЕР И МЕТОДА КУСТА СОБЫТИЙ ДЛЯ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Автоматизация различных процессов на предприятиях и в организациях и постоянное усложнение архитектуры информационных систем (ИС) являются предпосылками к появлению уязвимостей ИС, которые могут быть использованы злоумышленниками для реализации угроз безопасности информации. В настоящее время существует большое количество подходов к анализу и оценке угроз и рисков, характерных для ИС. В данной статье рассмотрены деревья атак-контрмер и метод куста событий – два графических подхода к оценке безопасности ИС, позволяющих в наглядном виде представить потенциальные атаки на систему и способы противодействия им. Приведен пример построения дерева атак-контрмер и куста событий для DDoS-атак, направленных на насыщение полосы пропускания ИС. Сформулированы критерии сравнения данных двух методов и на их основании проведен анализ применимости деревьев атак-контрмер и метода куста событий для оценки безопасности ИС.

Ключевые слова: *информационная система, информационная безопасность, деревья атак-контрмер, метод куста событий, оценка защищенности информационных систем.*

A COMPARATIVE STUDY OF ATTACK-DEFENSE TREES AND EVENT BUSH METHOD APPLICABILITY FOR INFORMATION SYSTEMS SECURITY ASSESSMENT

Automation of various processes at the enterprises and the area organizations and constant information systems architecture complication are the prerequisites for appearance of security vulnerabilities that can be exploited by adversaries. There is a great number of security threats and risks analysis and assessment approaches. In this article attack-defense trees and event bush method are considered. These methods are graphical security assessment approaches, allowing to describe potential attacks on the system and countermeasures to them. An example of attack-defense tree and event bush for DDoS attacks directed at information systems bandwidth saturation is given. The criteria for attack-defense trees and event bush method comparison are formulated. In accordance with the proposed criteria, the analysis of attack-defense trees and event bush method applicability in information systems security assessment is made.

Keywords: *information security, information system, attack-defense tree, event bush method, information systems security assessment.*

Информационная система (далее – ИС) представляет собой интегрированный набор компонентов для сбора, хранения и обработки данных и для предоставления информации, знаний и цифровых продуктов. Использование ИС позволило автоматизировать и ускорить решение различного рода задач, а информация и знания стали жизненно важными экономическими ресурсами. Внедрение информационных технологий постоянно открывают не только новые возможности, но и создают основу потенциальным угрозам. Развитие информационных и коммуникационных технологий привело к тому, что ИС находят все более широкое применение и в Российской Федерации. На федеральном уровне подготовлен ряд нормативно-правовых актов, регламентирующих вопросы использования данных технологий в органах государственной власти и органах местного самоуправления. Соответствующими органами разработаны методические рекомендации по предотвращению угроз ИС. Но, ввиду того, что в системном плане ИС представляет собой сложную организационно-техническую систему, характеризующуюся большим количеством разнородных параметров, становится актуальной задача анализа защищенности той или иной системы.

Защищенность информационных систем

В настоящее время вопросам оценки защищенности ИС посвящено большое количество отечественных и зарубежных публикаций. На этапе проектирования перспективным направлением в оценке защищенности ИС является представление возможностей нарушителей в виде деревьев и графов атак и вычисления на основе данного представления разнообразных метрик защищенности [1]. Деревья атак тесно связаны с графами атак, однако различие лежит в представлении состояний и действий. Центральная тема для исследований графов атак – последовательность событий [2]. Также могут применяться и иные графические подходы к моделированию возможных атак и угроз – с помощью сетей Байеса, сетей Петри, иерархиче-

ских моделей представления атак, а также с помощью метода куста событий.

Метод куста событий

Метод куста событий (англ. event bush), предложенный и разработанный [3] для того, чтобы показать поведение информации в динамических системах, находит все большее распространение и применение в различных областях наук [4]. В настоящее время метод составляет основу методологии инженерии динамических знаний и используется для разработки ее единой грамматики. Информационная модель предметной области описывается кустом событий как совокупность событий четырех типов, расположенных в определенном порядке и связанных специальными причинно-следственными связями (определяется как многопоточная структура – см. рис. 1), удовлетворяющих определенным условиям. В текстовой форме куст событий — это список определенных простых и сложных высказываний, но в отличие от метода ориентированных графов с применением прямых, косвенных, положительных и отрицательных связей узлы куста событий обозначают высказывания, а ребра (стрелки) – отношения между высказываниями, которые отражают отношения «причина – следствие» между сущностями, которые эти высказывания описывают.

Метод куста событий является перспективным методом описания динамических систем, обладающий логико-семантической строгостью. С помощью метода куста событий могут быть эффективно решены задачи описания всех возможных сценариев в рамках рассматриваемой системы; построения вероятностных моделей; накопления, обработки и хранения знаний; в т.ч. поиск скрытых взаимосвязей.

Деревья-атак контрмер

Понятие деревьев-атак контрмер (англ. attack-defense trees) впервые было введено в работе [5] и впоследствии получило широкое применение в качестве инструмента анализа сценариев атак на ИС. Деревья атак-контрмер представляют собой графический способ отображения взаимодействия между злоумышленником, атакующим ИС, и ее защитником, и позволяют изучить возможные способы атаки системы и необходимые механизмы для противодействия им. Данный подход устраняет ряд ограничений, которыми обладают деревья атак — в частности, позволяет рассмотреть сценарий чередования действий атакующего и защитника системы [6].

Дерево атак-контрмер представляет собой связный граф, не содержащий циклов и кратных ребер. Дерево атак-контрмер содержит узлы двух типов – узлы атак и узлы контрмер. Вершина дерева (корневой узел) обозначает конечную цель атакующего. Вершины, соединенные ребрами с корнем дерева, представляют собой действия злоумышленника, которые он предпринимает для достижения поставленной цели. Конечная вершина, из которой не выходит ни одного нового ребра, называется также листовым узлом или базовым действием (basic action) и представляет собой действие злоумышленника или защитную меру, которые не могут быть разложены на составляющие. Вершины, не являющиеся листовыми узлами или корнем, называются узлами ветвления. Узлы ветвления обозначаются как узлы «И» или «ИЛИ». Для того, чтобы действие узла «И» выполнялось, все исходящие из него вершины должны быть истинными – должно выполняться каждое действие из всей совокупности дочерних элементов узла ветвления. Истинное состояние узла «ИЛИ» достигается в случае, если хотя бы один из его дочерних элементов принимает истинное значение. Каждый узел, обозначающий действие злоумышленника, может иметь один дочерний узел противопо-

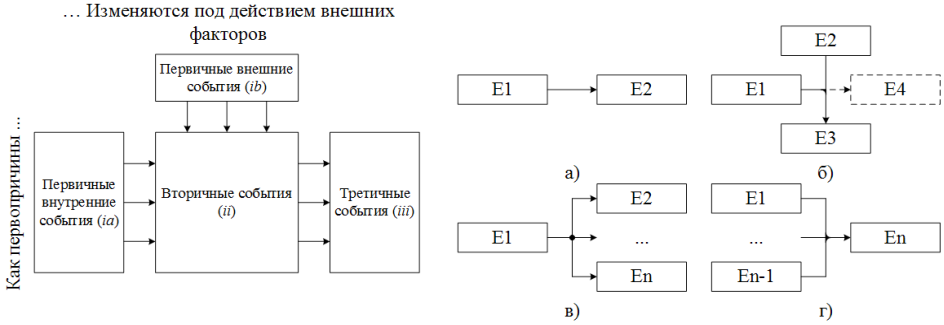

Рис. 1. Синтаксис базового блока куста событий и его соединительные элементы: поток (а), приток (б), разветвление (в) и слияние (г)

ложного типа – контрмеру. Узел контрмеры, в свою очередь, может иметь несколько уточняющих дочерних узлов и один дочерний узел, противопоставляемый защите [5].

Пример дерева атак-контрмер, построенного в программе ADTool 1.4, изображен на рис.2.

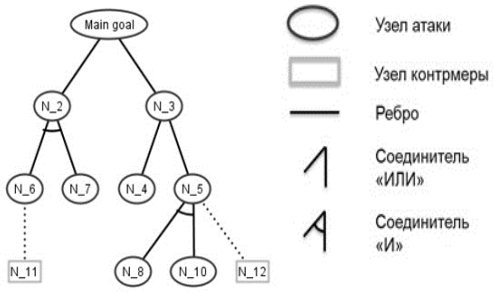

Рис. 2. Дерево атак-контрмер, построенное в программе ADTool 1.4

Построение дерева атак-контрмер и куста событий для анализа DDoS-атак, направленных на насыщение полосы пропускания ИС, и соответствующих мер их предотвращения

В данном разделе на рис. 3, 4 в форме дерева атак-контрмер и в форме куста событий представлены DDoS-атаки, использующие протоколы HTTP, ICMP, UDP, TCP, направленные на насыщение полосы пропускания, и соответствующие им контрмеры.

Для моделирования и анализа сценариев атак и защитных мер предназначен инструмент ADTool [7]. Данный инструмент позволяет создавать и редактировать деревья атак-контрмер, осуществлять расчет атрибутов дерева с помощью метода восходящего анализа, ранжировать атаки для определенных областей значений атрибутов и т.д. Кроме того, ADTool подходит для автоматизации и исследования всех разновидностей формализмов деревьев атак.

В данный момент времени метод куста событий не имеет конечного решения системы автоматизированного проектирования, однако, научными коллективами [8] активно разрабатывается интегрированная инженерная среда, позволяющая эффективно применять метод куста событий для решения широкого спектра задач научно-прикладного характера, среда, позволяющая применять метод в произвольных предметных областях, особенно таких, которые подразумевают обработку больших объемов информации и требуют серьезных вычислительных мощностей.

2. Наличие атрибутов, элементов присваивания и возможности построения пути от одного узла к другому.

Поскольку дерево атак-контрмер пред-

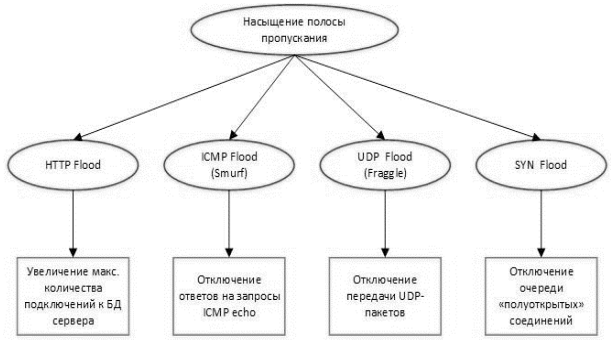

Рис. 3. DDoS-атаки и контрмеры в форме дерева атак-контрмер

Применимость деревьев атак-контрмер и метода куста событий для оценки безопасности информационных систем

В рамках данной статьи рассмотрена применимость деревьев атак-контрмер, как метода анализа ИС, по сравнению с методом куста событий.

Сравним особенности построения дерева атак-контрмер и куста событий для оценки безопасности ИС по следующим критериям:

1. Наличие или отсутствие систем автоматизированного проектирования для каждого из методов.

ставляет собой связный граф, не содержащий циклов и кратных ребер, путь между узлами представляет собой последовательность вершин, в которой каждая вершина соединена со следующей ребром, причем между парами вершин имеется только по одному пути. Моделирование шагов атаки с применением циклов возможно при использовании графов атак.

В отличие от деревьев, где путь может быть только один (от одного узла к другому) — у куста событий путь между узлами можно пройти разными путями.

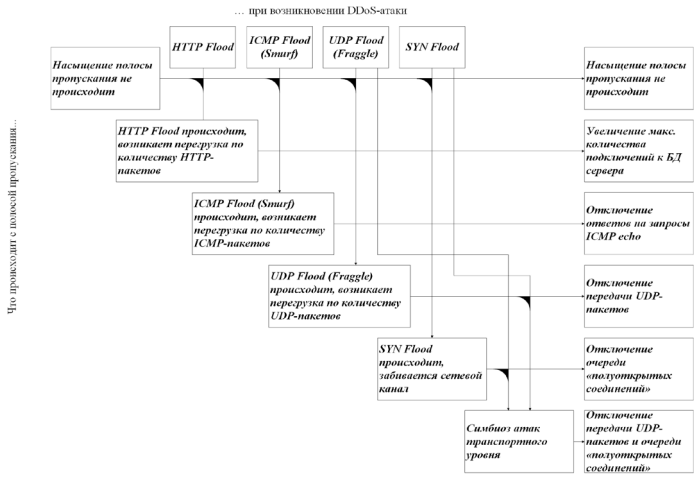

Рис. 4. DDoS-атаки и контрмеры в форме куста событий

3. Допустимость применения математического аппарата для каждого из методов.

Математический аппарат деревьев атак-контрмер был разработан в статье [5] для создания программного инструмента, позволяющего рассчитывать присваиваемые значения атрибутов листовым узлам деревьев атак-контрмер. Типы значений атрибутов зависят непосредственно от их содержания и могут принимать булевы значения, значения номинальной шкалы (низкий, средний, высокий), вещественные числа, а также дискретные и непрерывные распределения вероятностей [9].

Что касается математического аппарата, то стоит отметить то, что куст событий — вероятностная модель, представляющая собой множество событий и связей между ними и, следовательно, куст событий может быть использован для того, чтобы, например, вычислить вероятности неисправностей узлов аппаратуры по наличию или отсутствию ряда признаков основываясь на априори известных зависимостях между неисправностями и их проявлениями.

Заключение

Для подведения итогов необходимо разъяснить практический интерес описанной ранее модели, а также перспективы ее применения. Рассматриваемая модель, раскладывающая процесс DDoS-атак, направленных на насыщение полосы пропускания ИС, на минимально возможные единицы – простейшие действия, облегчает выявление потенциальных угроз развития событий на всех этапах этого процесса. Таким образом, ответственное должностное лицо за обеспечение безопасности ИС может проследить и заблаговременно выявить возможные потенциально слабые места. Здесь необходимо смотреть на эту ситуацию с разных сторон, наблюдать и моделировать, что может происходить при различных вариантах развития событий, тем самым предугадывая возможные действия. Соответственно, после этого разработать превентивные меры.

Стоит отметить то, что дерево атак-контрмер в отличии от куста событий – это в первую очередь инструмент аналитика, особенно на начальной стадии формулирования и выявлений требований к абстрактной ИС. С помощью деревьев атак-контрмер легко представляются схемы последовательных действий, при этом используется классический алгоритмический аппарат. Но в тоже время, в отличии от куста событий, дерево атак-контрмер имеет сложности в наглядности, если имеет место быть нескольким действиям.

Далее, если продолжить строить подобные модели одним и тем же методом, можно в результате прийти к формальной классификации информационных угроз в зависимости от свойств модели, описывающей каждый тип – наряду с теми сугубо утилитарными и не всегда безупречными классификациями, которыми сейчас описываются угрозы. А это выводит информационную безопасность на качественно новый уровень.

Литература

1. Котенко И.В., Степашкин М.В., Богданов В.С. Оценка безопасности компьютерных сетей на основе графов атак и качественных метрик защищенности // Тр. СПИИРАН. – 2006. –– Т. 2. – № 3. – С. 30-49.

2. Кляус Т.К., Гатчин Ю.А. Применение графического представления атак в моделировании угроз безопасности информации // Научно-технический вестник Поволжья. – 2017. – № 3. – С. 108-110.

3. Pshenichny C.A., Khrabrykh Z.V. Knowledge Base of Formation of Subaerial Eruption Unit // In S. Leroy I. Stuart (Eds.), Environmental Catastrophes and Recovery in the Holocene (Abstracts). London: Brunel University. URL: http://atlas-conferences.com/cgi-bin/abstract/caiq-22

4. Naumov A., Popov I., Bondarenko I., Krylov B., Timonin R., Ofitserov I. Dynamic Knowledge Representation as a Formalization Conveyor for Manmade Systems With Useful Impulse // Dynamic Knowledge Representaion in Scientific Domains. – 2018. – P. 270-285.

5. Kordy B., Mauw S., Radomirovic S., Schwietzer P. Foundations of attack-defense trees // Formal aspects of security and trust. – 2010. – Vol. 6561 of LNCS. – P. 1-16.

6. Кляус Т.К. Анализ состояния информационной безопасности систем электронного документооборота с помощью деревьев атак-контрмер // Сборник трудов IX Научно-практической конференции молодых ученых «Вычислительные системы и сети (Майоровские чтения)». – 2018. – С. 104-106.

7. ADTool [Электронный ресурс] // University of Luxembourg. URL: http://satoss.uni.lu/members/piotr/adtool/ (дата обращения: 23.05.2018)

8. Банькин А.А., Иванов Е.В. Метод куста событий // Сборник тезисов докладов конгресса молодых ученых (VIII Всероссийская межвузовская конференция молодых ученых, 12-15 апреля 2011 г.). – 2011. – № 1. – С. 3-4. URL: http://kmu.ifmo.ru/file/stat/12/kmu8_vep1.pdf (дата обращения: 23.05.2018)

9. Bagnato A., Kordy B., Meland P.H., Schwietzer P. Attribute decoration of attack-defense trees // International journal of secure software engineering. – 2012. – Vol. 3. – № 2. – P. 1-35.

References

1. Kotenko I. V., Stepashkin M. V., Bogdanov V. S. Evaluating Security of Computer Networks based on Attack Graphs and Qualitative Security Metrics [Ocenka bezopasnosti komp'juternyh setej na osnove grafov atak i kachestvennyh metrik zashhishhennosti]. Trudy SPIIRAN [SPIIRAS Proceedings], 2006, vol. 2, no.3, pp. 30-49.

2. Klyaus T.K., Gatchin Ju.A. The use of attacks graphical representation for threat modeling [Primenenie graficheskogo predstavlenija atak v modelirovanii ugroz bezopasnosti informacii]. Nauchno-tehnicheskij vestnik povolzh'ja [Scientific and technical bulletin of the Volga region], 2017, no. 3, pp. 108-110.

3. Pshenichny C.A., Khrabrykh Z.V. Knowledge Base of Formation of Subaerial Eruption Unit. Environmental Catastrophes and Recovery in the Holocene (Abstracts), London: Brunel University. Available at: http://atlas-conferences.com/cgi-bin/abstract/caiq-22.

4. Naumov A., Popov I., Bondarenko I., Krylov B., Timonin R., Ofitserov I. Dynamic Knowledge Representation as a Formalization Conveyor for Manmade Systems With Useful Impulse. Dynamic Knowledge Representaion in Scientific Domains, 2018, pp. 270-285.

5. Kordy B., Mauw S., Radomirovic S., Schwietzer P. Foundations of attack-defense trees. Formal aspects of security and trust, 2010, vol. 6561 of LNCS, pp. 1-16.

6. Klyaus T.K. Analyzing the information security of electronic document management systems using attack-defense trees [Analiz sostojanija informacionnoj bezopasnosti sistem elektronnogo dokumentooborota s pomoshh'ju derev'ev atak-kontrmer]. Sbornik trudov IX Nauchno-prakticheskoj konferencii molodyh uchenyh "Vychislitel'nye sistemy i seti (Majorovskie chtenija)" [Proceedings of the scientific and practical conference of young scientists "Computing systems and networks (Mayorov's readings)"], 2018, pp. 104-106.

7. ADTool. University of Luxembourg. Available at: http://satoss.uni.lu/members/piotr/adtool/.

8. Ban'kin A.A., Ivanov E.V. Event bush method [Metod kusta sobytij]. Sbornik tezisov dokladov konferenzii molodyh uchenyh [Proceedings of the young scientists' conference], 2011, no. 1, pp. 3-4. Available at: http://kmu.ifmo.ru/file/stat/12/kmu8_vep1.pdf.

9. Bagnato A., Kordy B., Meland P.H., Schwietzer P. Attribute decoration of attack-defense trees. International journal of secure software engineering, 2012, Vol. 3, no. 2, pp. 1-35.

КЛЯУС Татьяна Константиновна, аспирант кафедры «Проектирования и безопасности компьютерных систем» ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики». Россия, 197101, г. Санкт-Петербург, Кронверкский пр., д. 49. E-mail: t_klyaus@corp.ifmo.ru

НАУМОВ Андрей Дмитриевич, аспирант кафедры «Проектирования и безопасности компьютерных систем» ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики». Россия, 197101, г. Санкт-Петербург, Кронверкский пр., д. 49. E-mail: adnaumov@corp.ifmo.ru

ГАТЧИН Юрий Арменакович, доктор технических наук, профессор кафедры «Проектирования и безопасности компьютерных систем» ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики». Россия, 197101, г. Санкт-Петербург, Кронверкский пр., д. 49. E-mail: gatchin@mail.ifmo.ru

БОНДАРЕНКО Игорь Борисович, кандидат технических наук, доцент кафедры «Проектирования и безопасности компьютерных систем» ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики». Россия, 197101, г. Санкт-Петербург, Кронверкский пр., д. 49. E-mail: igorlitmo@rambler.ru

KLYAUS Tatiana, postgraduate student of the department of Design and Security of Computer Systems, ITMO University. Russia, 197101, Saint Petersburg, Kronverkskii avenue, 49. E-mail: t_klyaus@corp.ifmo.ru

NAUMOV Andrei, postgraduate student of the department of Design and Security of Computer Systems, ITMO University. Russia, 197101, Saint Petersburg, Kronverkskii avenue, 49. E-mail: adnaumov@corp.ifmo.ru

GATCHIN Yurii, doctor of technical sciences, professor of the department of Design and Security of Computer Systems, ITMO University. Russia, 197101, Saint Petersburg, Kronverkskii avenue, 49. E-mail: E-mail: gatchin@mail.ifmo.ru

BONDARENKO Igor, candidate of technical sciences, associate professor of the department of Design and Security of Computer Systems, ITMO University. Russia, 197101, Saint Petersburg, Kronverkskii avenue, 49. E-mail: igorlitmo@rambler.ru