ЧЕБЫШЕВСКИЙ СБОРНИК
Том 22. Выпуск 1.

УДК 519.7 DOI 10.22405/2226-8383-2021-22-1-488-494

Формальные модели безопасности

В. Л. Токарев (г. Тула)

Вячеслав Леонидович Токарев — доктор технических наук, профессор, Тульский государственный университет (г. Тула).
e-mail: tokarev22@yandex.ru

Аннотация

В статье излагается подход к построению формальной модели информационной безопасности, основанный на использовании алгебры предикатов. Модель представляется в виде дерева решений. Разработан и исследован алгоритм его построения, основанный на использовании дедуктивного метода поиска ответов.

Ключевые слова: алгебра предикатов, формальные модели, информационная безопасность.

Библиография: 18 названий.

Для цитирования:
В. Л. Токарев. Формальные модели безопасности // Чебышевский сборник, 2021, т. 22, вып. 1, с. 488–494.

CHEBYSHEVSKII SBORNIK
Vol. 22. No. 1.

UDC 519.7 DOI 10.22405/2226-8383-2021-22-1-488-494

Formal security models

V. L. Tokarev (Tula)

Vyacheslav Leonidovich Tokarev — doctor of technical sciences, professor, Tula State University (Tula).
e-mail: tokarev22@yandex.ru

Abstract

In paper describes an approach to building a formal model of information security based on the use of predicate algebra. The model is represented as a decision tree. The algorithm of its construction based on the deductive method of searching for answers is developed and investigated.

Keywords: predicate algebra, formal models, information security

Bibliography: 18 titles.

For citation:
V. L. Tokarev, 2021, "Formal security models" , *Chebyshevskii sbornik*, vol. 22, no. 1, pp. 488–494.

1. Введение

Согласно требованиям «Основных критериев оценки безопасности информационных технологий» [1], системы их защиты должны строиться на основе формальных моделей. Кроме того, соответствие системы защиты информации (СЗИ) в автоматизированных системах требованиям заданной политики безопасности может быть теоретически (то есть достаточно достоверно) обосновано только с использованием формальных моделей информационной безопасности, так как с их помощью можно доказать безопасность системы, опираясь на объективные доказуемые математические постулаты.

Формальные модели позволяют решить целый ряд задач, возникающих в ходе проектирования, разработки и сертификации АС в защищенном исполнении. Проблеме построения формальных моделей безопасности посвящен ряд работ, среди которых можно выделить две [2, 3], в которых рассматриваются модели для управления доступом к защищаемым ресурсам автоматизированных систем (АС). При этом модели предложено строить в виде отношений между субъектами и объектами АС, представляемых в виде графов и отображающих известные протоколы доступа [4].

В настоящем исследовании задача обеспечения информационной безопасности представляется как задача принятия решений в условиях наличия множества факторов, для поддержки решения которой может быть использован один из методов автоматического анализа данных - «дерево решений», использующийся в машинном обучении [5]. Известно, что построение таких деревьев позволяет не только корректно сформулировать задачу сложной структуры, но и получить множество вариантов решений [6]. Поэтому в качестве формальной модели информационной безопасности предлагается использовать «дерево решений» (ДР).

Обычно ДР имеют иерархическую структуру, состоящую из узлов, ветвей и листьев. Каждый лист представляет собой значение целевой переменной, изменяемое в ходе движения от корня к листу. Каждый внутренний узел соответствует одному из правил ветвления. Ветвям соответствуют атрибуты, от которых зависит целевая функция.

Автоматизация процесса построения ДР достигается тем, что правила ветвления генерируются путем обучения с использованием обучающих примеров [7]. В настоящее время разработано значительное число алгоритмов построения деревья решений: ID3, CART, C4.5, C5.0, NewId, ITrule, CHAID, CN2 и др.

Наибольшее распространение и популярность получили первые три: 1) ID3 (Iterative Dichotomizer 3) В его основе лежит рекурсивное разбиение обучающего множества, размещаемого в корневом узле дерева решений, на подмножества с помощью решающих правил [7, 8, 9]; 2) C4.5 — усовершенствованная версия алгоритма ID3, в которой была решена проблема переобучения и стала доступной обработка пропусков в обучающих данных [10, 11, 12]; 3) CART (Classification and Regression Tree) — алгоритм, обладающий расширенными возможностями обучения.

Эти и им подобные алгоритмы имеют широкий спектр применений: от робототехники [15, 16] до видеоигр [17] и управления беспилотниками [18]. Но, из-за того, что они реализуют индуктивный метод построения ДР, имеют общие недостатки:

1) чувствительность к шумам, обычно присутствующих в обучающих примерах;

2) разделяющие границы имеют определенные ограничения, снижающие качество ДР;

3) требуют большого объема обучающей выборки достоверных данных, что, по само по себе, может представлять проблему для ряда ситуаций, в которых приходится оперативно принимать решение.

Альтернативным способом автоматического построения ДР, выступающего в роли формальной модели безопасности, может быть дедуктивный метод. В данной статье исследуется использование этого подхода для построения формальной модели безопасности, а в качестве теоретической основы используется алгебра предикатов.

2. Алгоритм построения дерева решений

Предполагается, что: Предполагается, что: 1) формальная модель безопасности некоторого информационного ресурса может быть описана на языке логики предикатов; 2) задачу в конечном итоге можно свести к вопросу: a или b? (здесь a, b – различные решения, например, действия); 3) вопрос может быть представлен соответствующим предикатом ANS.

Тогда справедливы следующие утверждения.

Утверждение 1. *Совокупность предикатов, включающая предикаты-описания задачи и предикат-вопрос, путем применения метода резолюции, может быть представлена в форме дерева дизъюнктов (ДД), в котором листьям соответствуют исходные дизъюнкты, каждому узлу – образуемые резольвенты, а корню – дизъюнкт возможных решений, при этом переменные в дизъюнктах, полученных из исходных дизъюнктов переименовываются так, чтобы они не имели общих переменных.*

Утверждение 2. *Дерево дизъюнктов (ДД) может быть преобразовано в дерево решений (ДР) с помощью алгоритма ДДtoДР, основанного на методе резолюции.*

Теорема 1. *Алгоритм ДДtoДР, преобразующий ДД в ДР и позволяющий получить конкретный ответ (a или b), состоит из следующей последовательности шагов.*

1. В ДД определяются дизъюнкт $D = res(D_1, D_2)$ – резольвента дизъюнктов D_1 и D_2, с отрезаемыми литерами L_1 и L_2, соответственно, и и – наиболее общий унификатор литер L_1 и $\bar{L}_2$. После этого, ребро ДД, ведущее от D_i к $D, i = 1, 2$, помечается отрицанием литеры $L_i u$ и подстановкой и (если и – пустая подстановка, то остается только отрицание литеры $L_i u$).

2. Полученное ДД "переворачивается": корень оказывается наверху дерева (становится верхним узлом), а листья внизу, направление ребер – от корня к листьям. Устраняются все дизъюнкты, присвоенные узлам и помечаются все висячие вершины, например: $A, B, C, \ldots$

3. В полученном дереве удаляются все узлы (и связанные с ними ребра), соответствующие дизъюнктам, не содержащим предиката-вопроса ANS.

4. Выделяется дизъюнкт D_j, соответствующий j-ому висячему узлу. Для каждого висячего узла определяется конъюнкция литер $I(D_j)$, приписанных пути от верхнего узла до D_j и определяется дизъюнкт $C(D_j)$, соответствующий узлу D_j. В дизъюнкте-ответе отыскивается литера $L(D_j)$, являющаяся логическим следствием конъюнкции $D_j \wedge I(D_j)$ После этого литера $L(D_j)$ приписывается узлу D_j.

5. В полученном дереве остаются только такие i-е висячие узлы ($1 <= q$, где q – число уровней дерева) из которых ведет только одно ребро e_i и удаляются литеры , приписанные ребру e_i. Полученное дерево является искомым деревом решений.

Адекватность алгоритма решаемой задаче покажем на простом примере.

Пусть известны следующие правила: 1) если угроза информационной безопасности наиболее актуальна от внутреннего источника, то администратор безопасности (АБ) должен применить комплекс мер "a"; 2) если угроза безопасности наиболее актуальна от внешнего источника, то АБ должен применить комплекс мер "b"; 3) Вопрос: «какой комплекс мер должен применить АБ в настоящий момент времени?»

Пусть предикат P(x) означает: « x(АБ) знает, что в настоящий момент времени актуальна угроза внутренняя», предикат $R(x, y)$ – «x должен применить комплекс y». Тогда описание ситуации на языке алгебры предикатов принимает вид множества дизъюнктов:

1) $\bar{P}(x) \vee R(x, a)$; 2) $P(x) \vee R(x, b)$; 3) $\bar{R}(x, y) \vee ANS(y)$.

Из этого множества получим резольвенты для построения ДД:

4) $\bar{P}(x) \vee ANS(a)$ из дизъюнктов 1,3;

5) $P(x) \vee ANS(b)$ из дизъюнктов 2,3;

6) $ANS(a) \vee ANS(b)$ из дизъюнктов 4,5;

Формулам 1-6 соответствует дерево дизъюнктов (рис.1,а). Применение алгоритма ДДtoДР позволило получить дерево решений (рис.1,б).

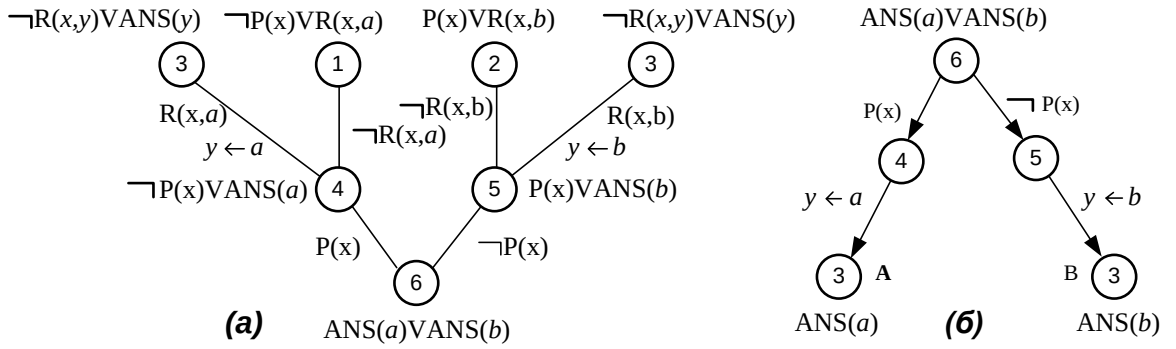

Рис. 1: Два дерева: а-дизъюнктов и б-решений

Доказательство. На шаге 4 предикат $ANS(a)$ приписан узлу A после того, как было показано, что $ANS(a)$ является логическим следствием конъюнкции
$P(x) \wedge R(x,a) \wedge (\bar{R}(x,y) \vee ANS(y))$, а так как дизъюнкт $\bar{R}(x,y) \vee ANS(y)$ входит в число входных дизъюнктов, то он истинен. Поэтому, предикат $ANS(a)$ истинен всегда, когда истинна конъюнкция $P(x) \wedge R(x,a)$. Показано, что предикат $R(x,a)$ является логическим следствием из $P(x)$ и дизъюнкта (1). Поэтому $R(x,a)$ должен быть истинен, если истинен предикат $P(x)$. Отсюда истинность предикатов $P(x)$ и $R(x,a)$ влечет истинность $ANS(a)$, тогда истинность $P(x)$ влечет истинность $ANS(a)$. Аналогично: истинность $\bar{P}(x)$ влечет истинность $ANS(b)$. Это доказывает корректность полученного дерева решений, а следовательно, и полученной модели безопасности.

3. Практический пример использования предложенного метода

Типичную схему получения доступа некоторого субъекта к объекту защищенной АС можно продемонстрировать следующим примером. Субъект s_i хочет получить доступ к объекту o_j, выдавая соответствующий запрос f_1. Команда, выполняя этап проверки b полномочий субъекта совершает действие f_2 – открывает доступ, если полномочия субъекта подтверждены, или действие f_3 - запрещает доступ, выдавая субъекту s_i соответствующее сообщение, если иначе. СЗИ должна определить, какое действие ей нужно совершить f_2 или f_3 в ответ на запрос f_1.

Введя предикат $P(s,x,q_k)$: "субъект s_i находится в точке a в состоянии q_k указанные правила представим в виде следующих формул алгебры предикатов:

1)$\bar{P}(s,a,q_k) \vee P(s,b,f_1(s,a,b,q_k))$;

2)$\bar{P}(s,b,q_k) \vee R(s) \vee P(s,c,f_2(s,b,c,q_{k+1}))$;

3)$\bar{P}(s,b,q_k) \vee R(s) \vee P(s,c,f3(s,b,a,q_k))$;

4)$P(s_i,c,q_{k+1})$;

5)$\bar{P}(s_i,c,q_{k+1}) \vee ANS(q_{k+1})$;

Из полученных дизъюнктов образуем резольвенты:

6)$\bar{P}(s,b,q_k) \vee R(s) \vee ANS(f_3(s,b,a,q_k))$ из дизъюнктов (3) и (5);

7)$\bar{P}(s,b,q_k) \vee \bar{R}(s) \vee ANS(f2(s,b,c,q_{k+1}))$ из дизъюнктов (2) и (5);

8)$\bar{P}(s,b,q_k) \vee ANS(f_3(s,b,a,q_k)) \vee ANS(f_2(s,b,c,q_{k+1}))$ из дизъюнктов (6) и (7);

9)$\bar{P}(s,b,q_k) \vee ANS(f_3(s,b,a,f_1(s,a,b,q_k))) \vee ANS(f_2(s,b,c,f_1(s,a,b,q_k))$ из дизъюнктов (1) и (8);

10)$ANS(f_3(s,b,a,f_1(s,a,b,q_k)) \vee ANS(f_2(s,b,c,f_1(s,a,b,q_k))$ из дизъюнктов (4) и (9).

Полученный 10-й дизъюнкт – это ответы, полученные из ДР по алгоритму ИКО: 1) Субъект s_i переходит из точки a в состоянии q_k в точку b с помощью запроса f_1, если отношение R содержит право доступа субъекта к объекту o_j, а система с помощью действия f_2 переходит в состояние q_{k+1}; 2) Иначе система с помощью действия f_3 возвращается в исходное состояние q_k и выдает сообщение субъекту s_i об отказе в доступе к объекту o_j.

Практика показала: 1) соответствие полученного ДР реальной задаче обнаружения нарушения правил доступа несанкционированного субъекта к объекту защищенной АС; 2) адекватность моделей, полученных предложенным методом, реальным правилам и протоколам, прописанным в политиках безопасности большинства защищенных автоматизированных систем.

4. Заключение

В работе предложен подход к построению формальных моделей информационной безопасности автоматизированных систем в форме дерева решений. Показано, что для повышения рациональности вырабатываемых на основе формальной модели решений, целесообразно выстраивать дерево решений не на основе широко используемого индуктивного метода (алгоритмы ID3, CART, C4.5, C5.0, NewId, ITrule, CHAID, CN2), а на основе дедуктивного метода поиска ответов, в качестве теоретической основы которого может быть использована алгебра предикатов.

На основе предложенного подхода разработан и исследован алгоритм построения дерева решений. Показана адекватность получаемых моделей существующим протоколам обеспечения информационной безопасности компьютерных систем.

Предложенный подход может стать теоретической основой для построения систем защиты информации автоматизированных систем с гарантированным качеством и для разработки более совершенных механизмов обеспечения информационной безопасности.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. ISO/1EC 15408-1: 2009 — Evaluation criteria for IT security — Part 1: Introduction and general model.

2. Девянин П.Н. О разработке моделей безопасности информационных потоков в компьютерных системах с ролевым управлением доступом. // Материалы 3-ей международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ им. М.В. Ломоносова. 25-27 октября 2007 г. – М.: МЦНМО, 2008. – с. 261-265.

3. Девянин П.Н. Проблема обоснования адекватности формальных моделей безопасности логического управления доступом и их реализации в компьютерных системах. // Системы высокой доступности. 2012, №2. – с. 45-49.

4. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2011. – 944 с.

5. Quinlan, J. R., Induction of Decision Trees. Machine Learning 1: 81-106, Kluwer Academic Publishers. 1986.

6. Kashnitsky Y. S. Methods of the search of accurate and interpretable rules for classifying data with complex structure //Proceedings of the conference КИИ-2016. In 3-t., Smolensk: publishing House «Универсум», 2016, 2, p.183-191, - 408c. (pdf)

7. Quinlan, J. R. “Probabilistic decision trees”. In: Y. Kodratoff and R. Michalski (Eds.), “Machine Learning. An Artificial Intelligence Approach”. Vol. III, Morgan Kaufmann Publishers, Inc., 1990. pp. 140–152

8. Iterative Dichotomizer 3 Grzymala-Busse, Jerzy W. "Selected Algorithms of Machine Learning from Examples"(PDF). 1993.

9. Taggart, A.J., DeSimone, A.M., Shih, J.S., Filloux, M.E. and Fairbrother, W.G. "Large-scale mapping of branchpoints in human transcripts in vivo". Nature Structural and Molecular Biology. 2012. pp.719–721.

10. Quinlan J. R. Learning With Continuous Classes // Proceedings of the 5th Australian Joint Conference on Artificial Intelligence. — 1992. — P. 343—348.

11. Quinlan J.R. C4.5 Programs for Machine Learning. Morgan Kaufmann, San Mateo, California, 1993.

12. Quinlan J.R. Improved Use of Continuous Attributes in C4.5 (англ.) // Journal of Artificial Intelligence Research. — 1996. — Vol. 4. — P. 77—90. — ISSN 1076-9757. — doi:10.1613/jair.279.

13. Breiman L., Friedman J.H., Olshen R.A., and Stone C.T. Classification and Regression Trees. Wadsworth, Belmont, California, 1984.

14. Machine Learning, Neural and Statistical Classification. Editors: D. Michie, D.J. Spiegelhalter, C.C. Taylor, 02/17/Journal of the American Statistical Association 1994.

15. Marzinotto, A.; Colledanchise, M.; Smith, C.; Ögren, P. "Towards a Unified BTs Framework for Robot Control"(PDF). Robotics and Automation (ICRA), 2014 IEEE International Conference.2014.

16. Colledanchise, M.; Ögren, P. Michele C. and Petter O.¨ Behavior Trees in Robotics and AI. 2018. CRC Press. arXiv:1709.00084. doi:10.1201/9780429489105. 3 Jun 2020. ISBN 978-1-138-59373-2. S2CID 27470659.

17. Ögren, Petter. "Increasing Modularity of UAV Control Systems using Computer Game Behavior Trees"(PDF). AIAA Guidance, Navigation and Control Conference, Minneapolis, Minnesota. 2012. pp. 13–16.

18. Klöckner, Andreas "Behavior Trees for UAV Mission Management". GI-Jahrestagung. 2013. pp. 57–68.

REFERENCES

1. “ISO/1EC 15408-1 2009 , Evaluation criteria for IT security, Part 1: Introduction and general model”.

2. Devyanin P. N. 2008, “On the development of security models for information flows in computer systems with role-based access control”, Materials of the 3rd international scientific conference on security and counteraction to terrorism. Lomonosov Moscow state University. 25-27 October 2007,Moscow: ICNMO,. - pp. 261-265.

3. Devyanin P. N. 2012, “The Problem of justification of adequacy of formal security models of logical access control and their implementation in computer systems”, High availability systems, no. 2, pp. 45-49.

4. Olifer V. G.& Olifer N. A. 2011, “Computer networks. Principles, technologies, and protocols” , St. Petersburg: Piter, 944 p.

5. Quinlan, J. R. 1986, “Induction of Decision Trees. Machine Learning 1”, Kluwer Academic Publishers, pp. 81-106.

6. Kashnitsky, Y. S. 2016, “Methods of the search of accurate and interpretable rules for classifying data with complex structure” ,XV artificial intelligence conference КИИ-2016 (Smolensk, Russia), Proceedings of the conference. In 3-t., Smolensk, Publishing House «Универсум», pp.183-191.

7. Quinlan, J. R. 1990, “Probabilistic decision trees”. In: Y. Kodratoff and R. Michalski (Eds.), “Machine Learning. An Artificial Intelligence Approach”. Vol. III, Morgan Kaufmann Publishers, Inc., pp. 140–152

8. Jerzy, W. GRZYMALA-BUSSE, 1993, "Selected Algorithms of Machine Learning from Examples". Department of Computer Science, University of Kansas, KS 66045, USA

9. Taggart A.J, DeSimone A.M, Shih J.S, Filloux M.E and Fairbrother W.G. 2012, "Large-scale mapping of branchpoints in human pre-mRNA Nat Struct Mol Biol. PMID: 22705790; PMCID: PMC3465671. pp.719–721.

10. Quinlan J. R. 1992, “Learning With Continuous Classes”, Proceedings of the 5th Australian Joint Conference on Artificial Intelligence. pp. 343—348.

11. J.R. Quinlan 1993, “Programs for Machine Learning”. Morgan Kaufmann, San Mateo, California.

12. Quinlan J.R. 1996, “Improved Use of Continuous Attributes in C4.5”, Journal of Artificial Intelligence Research. Vol. 4, pp. 77—90.

13. Breiman L., Friedman J.H. , Olshen R.A. and Stone C.T. 1984, “Classification and Regression Trees”. Wadsworth, Belmont, California.

14. Michie D., Spiegelhalter D.J., Taylor C.C. 1994, “Machine Learning, Neural and Statistical Classification”, 02,17, Journal of the American Statistical Association.

15. Marzinotto, Alejandro; Colledanchise, Michele; Smith, Christian; Ögren, Petter 2014, "Towards a Unified BTs Framework for Robot Control". Robotics and Automation (ICRA), IEEE International Conference.

16. Colledanchise, Michele; Ögren, Petter, Michele, Colledanchise and Petter, Ogren 2018, ‘Behavior Trees in Robotics and AI”. CRC Press. arXiv:1709.00084.3 Jun 2020.

17. Ögren, Petter 2012, "Increasing Modularity of UAV Control Systems using Computer Game Behavior Trees"(PDF). AIAA Guidance, Navigation and Control Conference, Minneapolis, Minnesota. pp. 13–16.

18. Klöckner, Andreas 2013, "Behavior Trees for UAV Mission Management". GI-Jahrestagung. pp. 57–68.

Получено 11.11.2020 г.
Принято в печать 21.02.2021 г.

ЧЕБЫШЕВСКИЙ СБОРНИК
Том 22. Выпуск 1.

УДК 512.542 DOI 10.22405/2226-8383-2021-22-1-495-501

Замечание о произведении двух формационных tcc-подгрупп[1]

А. А. Трофимук

Александр Александрович Трофимук — кандидат физико-математических наук, Брестский государственный университет им. А.С. Пушкина (Беларусь, г. Брест).
e-mail: alexander.trofimuk@gmail.com

Аннотация

Подгруппа A группы G называется *tcc-подгруппой* в G, если существует подгруппа T группы G такая, что $G = AT$ и для любого $X \leqslant A$ и $Y \leqslant T$ существует элемент $u \in \langle X, Y\rangle$ такой, что $XY^u \leq G$. Запись $H \leqslant G$ означает, что H является подгруппой группы G. В этой статье мы исследуем группу $G = AB$ при условии, что A и B являются tcc-подгруппами в G. Доказано, что такая группа G принадлежит $\mathfrak{F}$, если подгруппы A и B принадлежат $\mathfrak{F}$, где $\mathfrak{F}$ — насыщенная формация такая, что $\mathfrak{U} \subseteq \mathfrak{F}$. Здесь $\mathfrak{U}$ — формация всех сверхразрешимых групп.

Ключевые слова: сверхразрешимая группа, тотально перестановочное произведение, насыщенная формация, tcc-перестановочное произведение, tcc-подгруппа.

Библиография: 15 названий.

Для цитирования:
А. А. Трофимук. Замечание о произведении двух формационных tcc-подгрупп // Чебышевский сборник, 2021, т. 22, вып. 1, с. 495–501.

CHEBYSHEVSKII SBORNIK
Vol. 22. No. 1.

UDC 512.542 DOI 10.22405/2226-8383-2021-22-1-495-501

A remark on a product of two formational tcc-subgroups

A. A. Trofimuk

Alexander Alexandrovich Trofimuk — candidate of physical and mathematical sciences, Brest State A.S. Pushkin University (Belarus, Brest).
e-mail: alexander.trofimuk@gmail.com

[1]Исследование выполнено при финансовой поддержке Белорусского республиканского фонда фундаментальных исследований (проект Ф19РМ-071).