DOI 10.37882/2223-2966.2023.6-2.39

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КОНФЛИКТА СИСТЕМЫ ОБЛАКА И НАРУШИТЕЛЕЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

MATHEMATICAL MODEL OF THE CONFLICT OF THE CLOUD SYSTEM AND INFORMATION SECURITY VIOLATIONS

A. Tonkikh
E. Avksentieva

Summary: The problem of information systems security does not lose its relevance due to a significant increase in the number of information products on the market. In this paper, on the basis of mathematical modeling of conflict systems, a model has been developed for assessing the security of information in a cloud information system. It is based on the method of hybrid automata. Probabilistic equations are composed. The components of the cloud and the intruder are described, the assumptions and approximations are indicated.

Keywords: conflict, model, hybrid automaton, probability, cloud, intruder.

Тонких Андрей Сергеевич
Национальный исследовательский университет ИТМО
astonkikh@mail.ru
Авксентьева Елена Юрьевна
кандидат педагогических наук, доцент,
Национальный исследовательский университет ИТМО

Аннотация. Проблема безопасности информационных систем не теряет своей актуальности в связи со значительным ростом количества информационных продуктов на рынке. В данной работе на основе математического моделирования конфликтных систем разработана модель для оценки безопасности информации в облачной информационной системе. В основу положен метод гибридных автоматов. Составлены вероятностные уравнения. Описаны компоненты облака и нарушителя, обозначены допущения и приближения.

Ключевые слова: конфликт, модель, гибридный автомат, вероятность, облако, нарушитель.

Введение

Современная теория конфликта стремится построить концептуальную модель, связывающую объекты и факторы, и направлена на понимание рационального поведения сторон в конфликтных ситуациях [1]. В этой модели конфликт представляется в виде графа, который описывает состояния системы и переходы между ними. Различные исследования, такие как работы Радько Н.М., Губанова Д.А., Коцыняк М.А., Вакуленко А.А. и других, рассматривают разные подходы к математическому моделированию конфликта систем, используя сети Петри, теорию игр, теорию активных систем, вероятностные сети и теорию динамических систем [2–5]. Ещё одним подходом является использование полумарковских случайных процессов (ПСП), описанных в работах Радзиевского В.Г., Андреещева И.А. и Вялых А.С. [6–8]. Однако, для моделирования на основе ПСП требуется знание плотностей распределения вероятностей времени нахождения систем в состояниях, которые зачастую неизвестны. Кроме того, этот метод требует значительного времени для реализации. В данной работе используется метод формализма гибридных автоматов, где каждый объект в конфликте представлен диаграммой состояний, отражающей его поведение. Пример применения имитационного моделирования для оценки безопасности информации в облачной информационной системе рассмотрен в работе [9].

Описание математической модели конфликта систем

В конфликте систем есть две стороны. Первой стороной являются компоненты системы облака. Второй стороной выступает модель нарушителей. Если во время указанного диапазона времени $0 \le t \le T$ безопасность информации в компонентах системы облака обеспечена, то в конфликте выигрывают компоненты системы облака. Система облака должна быть в группе состояний, которая характерна для работы в стандартном режиме, считается, что в этой группе информация, находящаяся в компонентах облака, конфиденциальна, доступна и целостна. В случае преодоления злоумышленниками системы безопасности, компоненты облачной инфраструктуры перейдут в критическое состояние. Результат работы облачной инфраструктуры будет считаться отрицательным.

Вторая сторона конфликта — нарушители, способные скомпрометировать находящуюся в облаке информацию. В случае успеха нарушителей, который определяется переходом системы облака в критическое состояние за диапазон времени $0 \le t \le T$, считается, что нарушители выиграли в конфликте. В противном случае, если не удалось достигнуть результата в указанный диапазон времени, считается, что нарушители проиграли.

Модель конфликтного взаимодействия компонентов системы облака и нарушителей представлена на рис. 1.

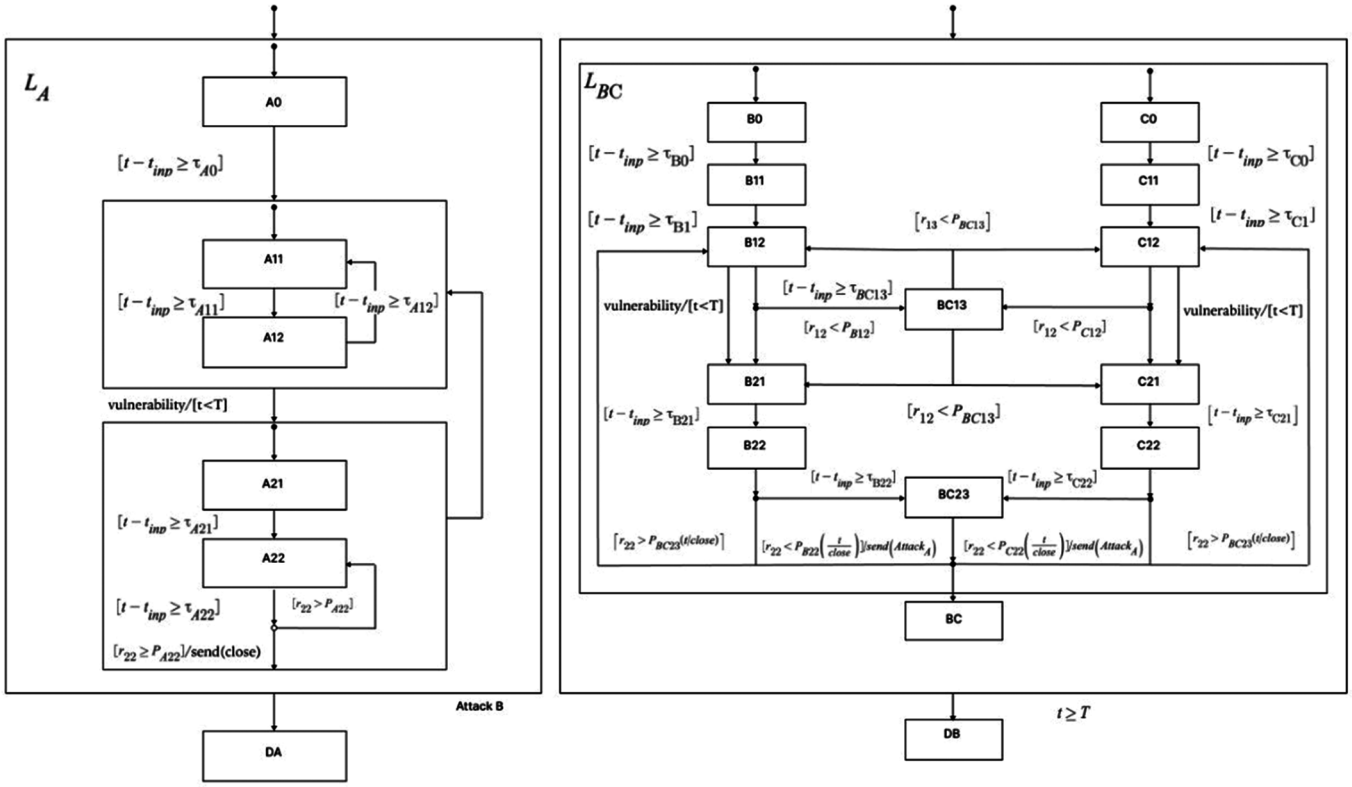

Рис. 1. Конфликт, представленный 3 гибридными автоматами

На рис. 1 представлен автомат, описывающий состояния системы облака (*A*), и автоматы (*B*) и (*C*), описывающие состояния, в которых находятся нарушители, так же между ними имеется возможность обмена информацией. Введем значение S^D, которое содержит основные состояния для системы облака и для системы нарушителей $S^D = \{s_a, s_{bc}\}$. Каждая из переменных s_a и s_b принимает значения $s_a \in Q_A = \{L_A, D_A\}$, $s_{bc} \in Q_{BC} = \{L_{BC}, D_{BC}\}$. Состояние компонентов системы облака обозначено группой L_A. Если компоненты находятся в этой группе до момента использования нарушителем имеющейся уязвимости, то автомат *A* переходит в критическое состояние. Использование уязвимости нарушителем приводит к переходу компонентов системы из состояния L_A в состояние D_A. Состояние, в рамках указанного диапазона времени которого автоматы *B* и *C* функционируют с целью нарушения работы *A*, обозначены группой L_{BC}. Работа состояния L_{BC}, в рамках указанного диапазона времени, приводит к поражению нарушителя и его переходу в состояние D_{BC}. Под влиянием событий *attack_BC* и $t \geq T$, определяющих поражение для компонентов системы облака и нарушителя совершается переход в состояния D_A для компонентов системы облака и состояние D_{BC} для нарушителя. Так же введём множества $Q = Q_A \times Q_{BC}$, $L = \{L_A, L_{BC}\}$, $D = \{D_A, D_{BC}\}$. Состояния из множества *D* в данной модели являются завершающими. Стрелки с черным кругом обозначают начальные состояния.

В данной модели существуют переходы двух типов: В обратном направлении — переход к предыдущему дискретному состоянию и в прямом — переход задаваемый последовательностью дискретных состояний.

В обобщённом виде поведение для любого из состояний на диапазоне времени $[t_{k-1} = t_{inp}, t_k = t_{out}]$, согласно [10–12], задаётся на основе указанных соотношений:

$$x(t) = \left(\tau(t), r(t), u(t)\right)^T = f\left(x\left(t_{k-1}\right), t\right), t_{k-1} = t_{inp},$$

$$x\left(t_{k-1}\right) = \left(\tau_k, r_k, t_{k-1} + \tau_k\right)^T$$

$$(\tau_k, r_k)^T : P_{A(BC)k}(\tau, r) = P_{A(BC)k}(r \,/\, \tau) P_{A(BC)k}(\tau), \qquad (1)$$

$$\tau(t) = \tau_k, r(t) = r_k, u(t) = u(t_{k-1}) - t, t \geq t_{k-1}, t_{out} = t_k = t : l(u(t) = 0),$$

где $x = (\tau, r, u)^T \in R^3$ набор действительных чисел, описывающих поведение для всех состояний, кроме конечного;

τ — время исполнения действия в конкретном состоянии;

r –результат выполнения действия;

u — функция, определяющая диапазон времени до момента окончания действия и нахождения в указанном состоянии;

$P_{A(BC)k}(\tau,r)$ — плотность распределения переменных τ и r (в общем случае статистически зависимые случайные величины);

τ_k — время дислокации в состоянии. Данное значение генерируется с помощью плотности распределения $P_{A(BC)k}(\tau)$, в заданном диапазоне значений, и определяется системой уравнений (1) при выходе из состояния. r_k — значение, отвечающее за результат вероятностного перехода. Это значение формируется на основе условной плотности распределения $P_{A(BC)k}(r/\tau_k)$.

Описание компонентов системы облака

Введём множество

$$S_A^D = \left\{ Q_{A0}^L \cup Q_{A1}^L \cup Q_{A2}^L \right\},$$

где Q_{A0}^L— группа состояний из одного состояния, обозначает этап подготовки создания защищенных сервисов. $Q_{A0}^L = \left\{ A_0 \right\}$;

Q_{A1}^L — группа из двух состояний, определяющая состояния активной работы системы в штатном режиме. $Q_{A1}^L = \left\{ A_{11}, A_{12} \right\}$. Состояние A_{11} обозначает работу и обслуживание системы в штатном режиме. A_{12} обозначает проведение штатных работ;

Q_{A2}^L — группа состояний из двух состояний, обозначает этап деятельности системы в случае появления уязвимости. $Q_{A2}^L = \left\{ A_{21}, A_{22} \right\}$. A_{21} обозначает процесс получения информации об уязвимости и её последующий анализ. A_{22} обозначает процесс закрытия уязвимости.

Состояние A_0 является базовым и выполняется единожды. Переход из этого состояния происходит после выполнения условия $\left[t - t_{inp} \geq \tau_{A0} \right]$.

Состояния A_{11}, A_{12} являются цикличными, это значит, что компоненты системы облака после попадания в эти состояния будут находиться там всё время, пока не будет открыта новая уязвимость. Переход из состояний A_{11}, A_{12} возможен, если нарушитель использует уязвимость или если время работы системы кончится. Выполнение переходов между A_{11}, A_{12} определяется условиями вида $\left[t - t_{inp} \geq \tau_{A11} \right]$, $\left[t - t_{inp} \geq \tau_{A12} \right]$. Кроме того, возможен переход в состояние A_{21} при появлении новой уязвимости (событие «vulnerability»), при условии, что уязвимость обнаружена во временном промежутке $[t; T)$.

Состояния A_{21}, A_{22} так же цикличны, они выполняются, пока система не закроет уязвимость, нарушитель не использует её или время работы системы не кончится. Выполнение переходов между A_{21}, A_{22} определяется условиями вида $\left[t - t_{inp} \geq \tau_{A21} \right]$, $\left[t - t_{inp} \geq \tau_{A22} \right]$. Переход из состояния A_{22} происходит поэтапно. Сначала после выполнения условия $\left[t - t_{inp} \geq \tau_{A22} \right]$ происходит промежуточный переход. Далее проверяется ещё одно условие $\left[r_{22} \geq P_{A22} \right]$, если условие выполняется, то происходит переход в состояние A_{11} и создаётся событие, на рис. 1 обозначенное как «send(close)», оповещающее о закрытии уязвимости, иначе происходит возврат в состояние A_{22}. Здесь P_{A22} вероятность, задаваемая в (1) $r(t) = r_k$ не зависит от времени.

После выхода из группы состояний Q_{A2}^L система либо возвращается в группу состояний Q_{A1}^L, либо переходит в соответствующее конечное состояние.

Описание системы нарушителей

Для системы нарушителей выделяется два типа действий: действия, затрагивающие один автомат, и действия, затрагивающие работу двух автоматов. При параллельной работе автоматов B и C вероятности находятся как суммы вероятностей совместных событий. Введена новая вероятность для действий, которые относятся к B и C.

Введём множество $S_{BC}^D = \left\{ Q_{B0}^L \cup Q_{C0}^L \cup Q_{BC1}^L \cup Q_{BC2}^L \right\}$,

где Q_{B0}^L и Q_{C0}^L — группа состояний из одного состояния, обозначает этап подготовительных действий для приведения системы нарушителей в рабочее состояние. $Q_{B0}^L = \left\{ B_0 \right\}$ и $Q_{C0}^L = \left\{ C_0 \right\}$;

Q_{BC1}^L — группа из трех состояний, указывающая на нахождение системы BC в режиме мониторинга и обнаружения уязвимостей $Q_{BC1}^L = \left\{ B_{11}, B_{12}, C_{12}, C_{11}, BC_{13} \right\}$. Состояние B_{11} и обозначает процесс сбора данных о компонентах системы облака. B_{12} и C_{12} обозначает процесс поиска уязвимостей в системе защиты компонентов облачной системы. Состояние BC_{13} обозначает процесс обмена данными, в результате которого производится сообщение о нахождении уязвимости одной из систем;

Q_{B2C}^L — группа состояний, состоящая из трех состояний, которая обозначает состояние деятельности системы BC после получения информации о новой уязвимости $Q_{BC2}^L = \left\{ B_{21}, B_{22}, C_{21}, C_{22}, BC_{23} \right\}$. B_{21} и C_{21} обозначает процесс анализа обнаруженной уязвимости. B_{22} и C_{22} обозначает процесс использования уязвимости. BC_{23} обозначает процесс обмена данными, при котором сообщается использована ли уязвимость хотя бы одной из систем.

Состояния B_0, B_{11}, C_0, C_{11} являются базовыми и каждое из них ограничено единственным выполнением.

Переход из состояния B_0 происходит при выполнении условия $\left[t - t_{inp} \geq \tau_{B0} \right]$. Переход из состояния C_0 при выполнении условия $\left[t - t_{inp} \geq \tau_{C0} \right]$.

Выполнение переходов между B_{11}, B_{12} определяется условиями вида $\left[t - t_{inp} \geq \tau_{B11} \right]$, $\left[t - t_{inp} \geq \tau_{B12} \right]$. Так же для автомата *C*. Переход из состояний B_{12}, C_{12} начинается с проверки условия $\left[t - t_{inp} \geq \tau_{B12} \right]$, $\left[t - t_{inp} \geq \tau_{C12} \right]$. Далее проверяются условия $\left[r_{12} < P_{B12} \right]$ и $\left[r_{12} < P_{C12} \right]$, в случае выполнения этого условия происходит переход в состояние B_{21}, C_{21}, в противном случае переход будет выполнен в состояние BC_{13}. $\left[t - t_{inp} \geq \tau_{BC13} \right]$, далее проверяется условие $\left[r_{13} < P_{BC13} \right]$. Если условие выполнено, то производится переход в состояние B_{21}, C_{21}. В противном случае перехода не случится. Здесь P_{B12}, P_{C12} и P_{BC13} — вероятности, задаваемые в (1) $r(t) = r_k$ не зависят от времени. Вероятности P_{B12}, P_{C12} — учитываются при сложении совместных событий, P_{BC13} — вероятность события, несовместного с P_{B12}, P_{C12}. Также переход из состояния поиска уязвимостей в системе защиты компонентов системы облака в состояние анализа обнаруженной уязвимости, возможен при появлении новой уязвимости (обозначается как «vulnerability»), которая возникает на отрезке времени [*t*, *T*).

Выполнение переходов между $B_{21,}$ B_{22} определяется условиями вида $[t - t_{inp} \geq \tau_{B21}]$, $[t - t_{inp} \geq \tau_{B22}]$. Так же для системы *C*. Переход из состояния B_{22} начинается с проверки условия $[t - t_{inp} \geq \tau_{B22}]$. Так же для системы *C*. Далее проверяется условия $\left[r_{22} \geq P_{B22} \right]$ и $\left[r_{22} \geq P_{C22} \right]$. Если выполнено одно или два условия, то происходит событие «send(attack_A)», которое переводит компоненты системы облака в конечное состояние D_A. Если же условие не выполняется, то происходит переход в состояние B_{23}. $[t - t_{inp} \geq \tau_{B22}]$ действует данное условие и проверяется $\left[r_{22} \geq P_{BC23} \right]$. Выполнение условия означает успешное использование уязвимости одной из сторон. Здесь P_{B22}, P_{C22} и P_{BC23} вероятности, задаваемые в (1) $r(t) = r_k$, не зависят от времени.

Условие перехода из состояния B_{22} в состояние B_{12} (аналогично для автомата *C*) определяется вероятностью P_{B22}(t/close), зависящей от успеха деятельности компонентов системы облака:

$$P_{B22}\left(t \;/\; close\right) = \begin{cases} P_{bv}, t < t_{close}, \\ 0, t \geq t_{close}, \end{cases}$$

где t_{close} — время закрытия уязвимости;

P_{bv} — вероятность успеха нарушителя, когда выполняется этап обработки информации о появившейся уязвимости.

Заключение

В результате, разработана и описана модель конфликтной системы, состоящая из трех гибридных автоматов, один из которых представляет облако, два других — нарушителей системы безопасности. Была получена система вероятностных уравнений, которая позволяет моделировать вероятность успеха нарушителя для определенных допущений и приближений.

ЛИТЕРАТУРА

1. Grzyl B., Apollo M., Kristowski A. Application of game theory to conflict management in a construction contract // Sustainability. — 2019. — Т. 11. — №. 7. — С. 1983.
2. Гончаров А.А. и др. Развитие методов и построение алгоритмов поиска и классификации деструктивного контента, циркулирующего в социальной сети // Информация и безопасность. — 2019. — Т. 22. — №. 3. — С. 345–360.
3. Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. Модели репутации и информационного управления в социальных сетях // Управление большими системами: сборник трудов. — 2009. — №. 26-1. — С. 209–234.
4. Коцыняк М.А. и др. Методика оценки защищенности информационно-телекоммуникационной сети в условиях информационного противодействия // Радиолокация, навигация, связь. — 2017. — С. 83–89.
5. Вакуленко А.А., Шевчук В.И. Математическая модель динамики конфликта радиоэлектронных систем // Радиотехника. — 2011. — №. 1. — С. 56–59.
6. Радзиевский В.Г., Сирота А.А. Теоретические основы радиоэлектронной разведки. 2-е изд, испр. и доп. (1-е издание «Информационное обеспечение радиоэлектронных систем в условиях конфликта») — М. «Радиотехника», 2004 — 432 с.
7. Андреещев И.А., Будников С.А., Пиндус Я.М. Полумарковская модель оценки надежности функционирования информационно-телекоммуникационных систем в органах внутренних дел // Охрана, безопасность, связь. — 2016. — №. 1–2. — С. 41–48.
8. Вялых А.С., Вялых С.А. Динамика уязвимостей в современных защищенных информационных системах // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. — 2011. — №. 2. — С. 59–63.
9. Сирота А.А., Гончаров Н.И. Модели информационных процессов нессиметричного конфликтного взаимодействия систем и их применение в задачах исследования безопасности использования облачных технологий //Вестник ВГУ. Серия: Системный анализ и информационные технологии. — 2018. — №. 3. — С. 103–118.
10. Сирота А.А., Гончаров Н.И. Исследование конфликта коалиций систем с использованием формализма гибридных автоматов // Вестник воронежского государственного университета. Серия: Системный анализ и информационные технологии. — 2017. — №. 4. — С. 56–70.
11. Смирнов А.В. и др. Онтологический подход к организации взаимодействия сервисов интеллектуального пространства при управлении гибридными системами // Искусственный интеллект и принятие решений. — 2014. — №. 4. — С. 42–51.
12. Сирота А.А., Гончаров Н.И. Исследование конфликтных взаимодействий систем с использованием формализма гибридных автоматов // Математическое моделирование и информационные технологии в инженерных и бизнес-приложениях. — 2018. — С. 313–332.

Журнал «Современная наука: актуальные проблемы теории и практики»