УДК 004.056.5

АЛГОРИТМИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ТАБЛИЦ ФУНКЦИОНИРОВАНИЯ

[1]И.Х.Норматов, [2]Р.Н.Дадажанов, [3]М.Н.Атаджанов,
[1]Национальный университет Узбекистана имени Мирзо Улугбека, Ташкент, Узбекистан
[2]Университет общественной безопасности Республики Узбекистан, Ташкент, Узбекистан
[3]Военно-академический лицей имени Джалолиддина Мангуберди, Ургенч, Узбекистан

Аннотация. В статье рассматриваются вопросы обеспечения информационной безопасности систем обработки и хранения конфиденциальной информации. Предлагается алгоритмическая модель анализа защищенности информационных систем на основе динамических таблиц функционирования. Рассматриваются особенности управления и контроля потоков данных, а также методы оценки уровня защиты информационных ресурсов. Алгоритмическая модель используется как математический аппарат для моделирования динамических дискретных систем и позволяет выявлять уязвимости в функционировании системы защиты. Применение предложенного подхода обеспечивает более эффективное исследование состояния информационной

безопасности и повышение надежности систем защиты конфиденциальной информации.
Ключевые слова: информационная безопасность, защита конфиденциальной информации, алгоритмическая модель, таблицы функционирования, информационные системы, анализ защищенности, динамические системы, обработка данных, безопасность информации.

ALGORITHMIC MODEL OF INFORMATION SECURITY BASED ON FUNCTIONING TABLES

[1]I.Kh. Normatov, [2]R.N. Dadazhanov, [3]M.N. Atadzhanov
[1]National University of Uzbekistan named after Mirzo Ulugbek, Tashkent, Uzbekistan
[2]University of public safety of the republic of Uzbekistan, Tashkent, Uzbekistan
[3]Military academic lyceum named after Jaloladdin Manguberdi, Urgench, Uzbekistan

Abstract. Ensuring the security of information systems that process and store confidential data is an important task in modern digital infrastructures. This paper presents an algorithmic model of information security based on functioning tables. The proposed approach allows the formal description of information processes and the analysis of system states in the context of security control. Functioning tables are used as a mathematical tool for modeling the behavior of dynamic discrete systems and evaluating the effectiveness of security mechanisms. The developed model makes it possible to analyze information flows, identify potential vulnerabilities, and assess the reliability of protection mechanisms in information systems. The results of the study demonstrate that the use of functioning tables improves the efficiency of security analysis and provides a systematic approach to the protection of confidential information.
Keywords: information security, algorithmic model, functioning tables, confidential information protection, information systems, security analysis, data flow control.

Введение

Развитие информационных систем обработки и хранения конфиденциальной информации диктует необходимость построения надежной системы защиты конфиденциальной информации (СЗКИ).

В данной работе рассматриваются особенности работы с потоками данных, управление и контроль над ними, приводятся математические решения оценки защиты информационных ресурсов и различные аспекты оценивания экономической эффективности обеспечения конфиденциальности информационных ресурсов. Предлагается один из способов анализа защищенности системы – построение динамических таблиц функционирования (ТФ) информационной системы. С помощью алгоритмической модели на основе ТФ проводится обследование функционирования реализуемой системы защиты, и выявляются ее недостатки. В работе алгоритмические модели на основе ТФ используются

как математический аппарат для моделирования динамических дискретных систем [1–8].

Безопасность – это отсутствие опасности или наличие возможности надежно защититься от нее. Опасным следует считать такое информационное воздействие, которое чревато дестабилизирующим, деструктивным, ущемляющим интересы личности или страны и т.д. результатом.

Информационная безопасность общества, государства – это состояние либо отсутствия информационных угроз, либо, при наличии таковых, состояние защищенности и, следовательно, устойчивости основных сфер жизнедеятельности (политики, экономики, науки, техносферы, сферы государственного управления, культуры, военного дела, общественного сознания и т.д.) по отношению к опасным информационным воздействиям, причем как внедрению, так и извлечению информации.

Системный подход к информационной безопасности (ИБ) требует выделять ее субъекты, средства и объекты, принципы обеспечения, источники опасности, направленность опасных информационных потоков.

Эволюция информационных технологий (ИТ) связана с интеллектуальными системами, в которых присутствуют процессы зарождения, адаптации и развития. Системный подход определяет методологию и принципы построения систем ИТ. Принцип возможности моделирования позволяет предотвратить ошибки проектирования кибернетических систем. Принцип связности при разработке эффективной системы рассматривает объект защиты комплексно, объединяя объект защиты, внешнюю среду, средства защиты и угрозы злоумышленника и учитывая взаимосвязи: источник угрозы – фактор (уязвимость) – угроза (действие) – последствия (атака).

Построение системы защиты является обязательным условием для обеспечения безопасности конфиденциальной информации, хранимой и обрабатываемой в информационной системе. Требования к системе защиты информации формируются по результатам проведения обследования информационной системы и ориентированы на нейтрализацию уязвимостей системы. Одним из способов анализа защищенности системы является построение динамических таблиц функционирования (ТФ) информационной системы на базе сетей Петри [20]. С помощью алгоритмической модели на основе ТФ проводится обследование функционирования реализованной системы защиты, и выявляются ее недостатки.

Развитие информационных систем обработки и хранения

конфиденциальной информации диктует необходимость построения надежной системы защиты конфиденциальной информации (СЗКИ).

Построение СЗКИ проводится в несколько этапов. Первым этапом является обследование информационной системы (ИС), в рамках которого анализируется технология обработки, хранения и защиты информации, формируется модель нарушителя и модель угроз безопасности конфиденциальной информации (КИ), а также составляются требования к СЗКИ.

Требования к СЗКИ, в зависимости от вида КИ определяются согласно нормативно-законодательной базы Республики Узбекистан.

Алгоритмические модели на основе ТФ используются как математический аппарат для моделирования динамических дискретных систем

Моделирование на основе ТФ осуществляется на событийном уровне. Определяются, какие действия происходят в системе, какие состояния предшествовали этим действиям и какие состояния примет система после выполнения действия. Выполнение событийной модели в ТФ описывает поведение системы. На основе анализа результатов выполнения можно сказать о возможных состояниях системы, и при этом какие состояния в принципе не достижимы.

Основная часть

Таким образом, $ТФ = \{X, Y, A, O, \Theta, T, U, S, F, P\}$ – алгоритмическая модель АСУ обеспечения безопасности ИС, а также предотвращения любого вида угроз к ИС и информационным ресурсам (ИР), где

Y – множество возможных угроз O_j, $Y = \{O_j\}$;

X – множество решений предотвращения угроз A_i, $X = \{A_i\}$;

A – определенное решение предотвращения угроз;

O – определенное действие угроз;

Θ –множество координат Θ_{ij} соответствия A_i и O_j, $\Theta = \{\Theta_{ij}\}$;

T – время предотвращения и успешной реализации угрозы;

U – внешнее воздействие на $\{A_i:O_j\}$ по координате Θ_{ij} ;

S – множество переходов S_{ij} (переход из одной Θ_{ij} на другую $\Theta_{i+n, j+m}$);

$F(t)$ –функция изменения таблицы функционирования во времени;

P – множество вычислительных и логических операций ввода, вывода и управления;

Z – множество привилегий.

Если $\forall t_i \in T$ функция $F(t_i) = \text{const}$, то такая таблица функционирования называется статической (стационарной). Функция $F(t)$, задающая

изменения таблицы функционирования, называется функцией управления агрегатной системой или функцией планирования процессов в системе.

В каждый интервал времени t_i описание ТФ представляется в виде маркированной сети Петри: $M = \{P, D, I, O, \mu\}$, где P, D, I, O - соответственно, множества позиций (состояний), операций (переходов), входных и выходных состояний; μ-функция, отображающая множество позиций в множестве натуральных чисел $N: \mu: P \to N$. Каждая маркировка μ может быть представлена как вектор $\mu = (\mu_1, \ldots, \mu_n)$, здесь $n = |P| u \forall \mu_i \in N, i = \overline{1,n}$. Вектор μ определяет для каждой позиции P_i сети количество фишек, т.е. для $\mu_i, Pi, i = \overline{1,n}$ выполняется $\mu(Pi) = \mu_i$ Интервалы времени, в течение которых сеть Петри не изменяется, будем называть технологическими циклами (ТЦ) [1,3].

Таким образом, за неделимый элемент динамических дискретных систем принято рабочее место (РМ), соответствующее α_i определенному решению предотвращения угроз. Обозначим его через α_i, а множество РМ -через А. Каждое α_i может быть представлено в виде работников, работника плюс машины или машины. Каждое α_i имеет входы x и выходы y, внутреннее z состояние. На входы передаются сигналы (информация) или материалы в виде продуктов, веществ (жидких или газообразных) и т. д. Некоторые входные воздействия сигналов могут быть управляющими (g). В качестве машин применяются станки и вычислительные машины. Машины выступают в качестве орудия труда, а информация, материалы – в качестве предметов труда.

Рабочее место α_i соответствует агрегату Н.П. Бусленко. Каждому агрегату приписывается определенное количество операций d. Множество операций α_i обозначим через D. Кроме того, они функционируют во времени и имеют пространственные координаты. Множество РМ соединяются между собой дугами и образуют коммуникационную сеть с потоками α (имеется в виду потоки информации, веществ, а также транспортные, людские потоки и т.д.).

Так, система представляется в виде коммуникационной сети, вершины которой изображают РМ, способные выполнять определенное количество операций (решение задач, переработка материалов и т.д.), а дуги соответствуют потокам между этими местами. Такую сеть назовем R-сетью.

В процессе функционирования системы структура сети со временем может меняться: старые дуги и вершины аннулируются, а новые добавляются. Такие сети назовем ситуационными или RC-сетями. При решении определенного класса задач в течение времени (t_1, t_2) на каждом α выполняется одна из приписанных ему операций. Поэтому построение

самой сети и определение приписанной операции является основной задачей системных исследований. В определенный промежуток времени сеть можно изобразить в виде ориентированного графа неизменной структуры (рис. 1). Такое представление соответствует определению таблицы функционирования, и *R*-, *RC* сети представляются в виде ТФ. На этой сети можно фиксировать параметры потока и режим работы сети во времени [1, 2].

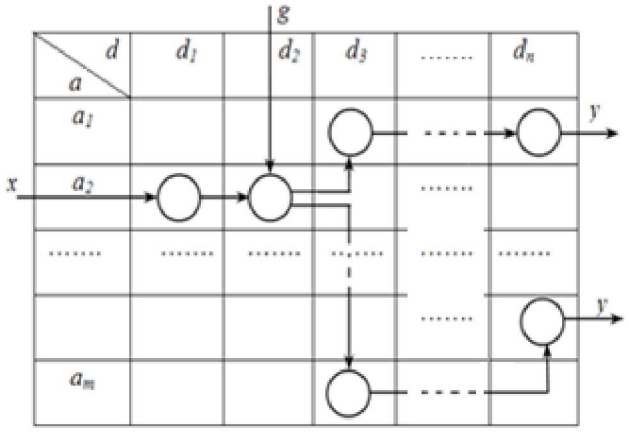

Рис. 1. ТФ гипотетического объекта управления
Fig. 1. TF of a hypothetical control object.

Воспользуясь системами действий сетей Петри мы создадим блок схему СЗКИ (рис. 2) и гибридный вариант сетей Петри в обеспечении ИБ. В блок схеме основным шагам является обнаружение угрозы Oj из множества Y. После идентификации угрозы O_j она проверяется общим архивом (П+И) просмотренных угроз. Если такие угрозы были рассмотрены ранее они обезвреживаются соответственными действиями $\{P_{ij}\ F\}$. Если угроза рассматривается первые тогда она анализируется и вычисляется $\{Y, P_{ij}, U_{ij}, T_{ij}, O_j, A_i\}$. Если после анализа источника $Y+Z$ и анализа привилегии Z_k угрозы не обнаружатся тогда они пересматриваются как $Y+Z_k$. После этого добавляются в архив пропущенных угроз П. Если при анализе и вычислении угрозы обнаружатся, то тогда действия будут идти по блок схеме № 1, Продолжение. Здесь после всех шагов угрозы добавляются в архив для быстрого обнаружения и идентификации угроз (рис. 2).

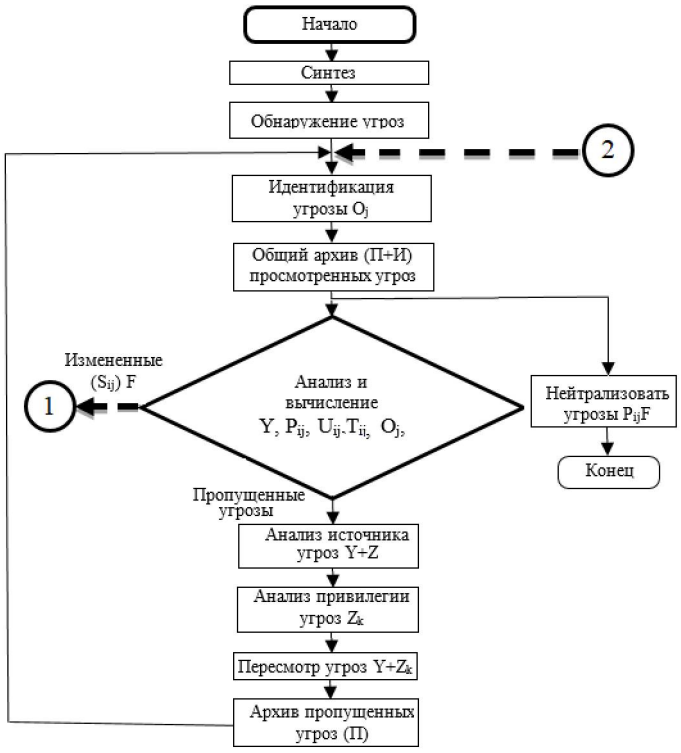

Рис. 2. Алгоритм работы ТФ № 1 (продолжение)
Fig. 2. Tables of fuctioning operation algorithm No. 1 (continued)

Рис. 3. Схема построения алгоритмической модели СКЗИ на основе ТФ
Fig. 3. The scheme of constructing an algorithmic model of the means of confidentional information protection based on tables of fuctioning

На рис. 3 в таблице функционирования представлены множество угроз $\{O_j\}$, а также множество действий $\{A_i\}$ для предотвращения угроз. Для функционирования данной ТФ необходимо в каждой ячейке было предоставлено минимум 3 входа: сама угроза; способы предотвращения

данной угрозы; привилегия пользователя в данной ситуации (например – системный администратор и пользователи разных уровней).

После обработки действия в ячейке (A_2 O_2) по формуле $\theta_{ij}=\{Y, P_{ij}, U_{ij}, T_{ij}, O_j, A_i, Z_k\}$ состояние угрозы меняется исходя из своей сущности и скрипта кода, после этого управление передается в другую ячейку. В нашем случае в (A_3 , O_3). Переход осуществляется по формуле $\{S_{ij}, F\}$.

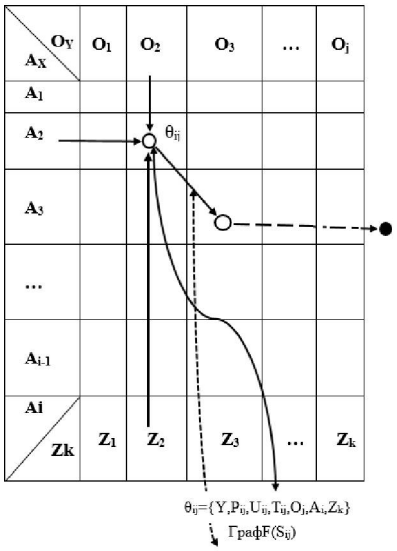

Рис. 4. Таблица функционирование СЗКИ
Fig. 4. Table of functioning the means of confidentional information protection

После окончания обработки угроза выводится из таблицы, т.е. уничтожается или добавляется в архив. При этом нужно учитывать то, что алгоритм работы ТФ № 1 является гибким и всегда может изменяться при обработке данных и будет совершенствоваться. Это отразится и на ТФ, которая будет постоянно дополняться новыми критериями. Эти действия в сетях Петри представлены в таблице на рис. 4.

Анализируя вышеотмеченные выводы и полученную таблицу функционирования, можно сконструировать для определенной внешней угрозы на систему пути вычисления, анализа и график работы в предлагаемой нами сети СЗКИ.

Заключение

Предложена алгоритмическая модель информационной безопасности на основе таблиц функционирования. Алгоритмический метод на основе таблицы функционирования использован как математический аппарат для моделирования динамических дискретных систем обнаружения и обезвреживания угроз при обеспечении защиты информации. Разработан метод оценки рисков информационной безопасности и обеспечения конфиденциальности информационных ресурсов. Предложен один из способов анализа защищенности системы – построение динамических

таблиц функционирования. Предложены математические решения оценки защиты информационных ресурсов и различные аспекты оценивания экономической эффективности обеспечения конфиденциальности информационных ресурсов.

Список использованных источников

1. Питерсон Дж. Теория сетей Петри и моделирование систем. М.: Мир, 1984.

2. Поспелов Г.С. Системный анализ и искусственный интеллект// Проблемы вычислительной техники. М.: Международный центр науки и техн. информ., 1981. С. 21–42.

3. Самарский А.А., Михайлов А.П. Математическое моделирование: Идеи. Методы. Примеры. М.: Физматлит, 2001.

4. Кабулов А.В. Норматов И.Х., Каландаров И.И. Алгоритмический подход управления сложными системами на примере производственных систем // ДАН АН РУз, г.Ташкент. 2017. № 1. С. 33–35.

5. Kabulov A.V., Normatov I.X., Kalandarov I.I., Karimov A.A. Algorithmic Method of Organization of Specialized Workshops // International Journal of Advanced Research in Science, Engineering and Technology. 2018. Vol. 5, iss. 4. P. 5670–5675.

6. Норматов И.Х. Алгоритм обнаружения и обезвреживания угроз на основе таблиц функционирования // IV Международный Косыгинский Форум «Проблемы инженерных наук: формирование технологического суверенитета». Сборник научных трудов Международного научно-технического симпозиума «Современные инженерные проблемы ключевых отраслей экономики страны» (20–22 февраля 2024 г.). Том 1. М.: РГУ им. А.Н. Косыгина, 2024. С. 78–84.

7. Норматов И.Х., Атажанов М.Н. Эффективност применения искусственного интеллекта (Artificial intelligence (AI)) в образователном процессе // International scientific and practical Conference of students, undergraduates, doctoral students and young scientists «Student, science and Innovation: modem research trends» dedicated to the Day of Science workers and the 125th anniversary of Kanysh Satpayev, 10 April 2024.

8. Normatov I., Atazhanov M., Karimov R. Development of an algorithmic system for detecting and disarming threats based on functioning tables // Технические средства защиты информатsiи: материалы XXIII Международной научно-технической конференции, Минск, 08 апреля 2025 года / Белорусский государственный университет информатики и радиоэлектроники [и др.]; редкол.: О. В. Бойправ [и др.]. Минск, 2025. С. 22–26.

References

1. Peterson J. Petri Net Theory and Systems Modeling. Moscow: Mir, 1984. (In Russian)

2. Pospelov G.S. Systems Analysis and Artificial Intelligence// Problems of Computer Engineering. Moscow: International Center for Science and Technical Information, 1981. pp. 21–42. (In Russian)

3. Samarskii A.A., Mikhailov A.P. Mathematical Modeling: Ideas. Methods. Examples. Moscow: Fizmatlit, 2001. (In Russian)

4. Kabulov A.V., Normatov I.Kh., Kalandarov I.I. An Algorithmic Approach to Controlling Complex Systems Using Production Systems as an Example // DAN AS RUz, Tashkent. 2017. No. 1. pp. 33–35. (In Russian)

5. Kabulov A.V., Normatov I.Kh., Kalandarov I.I., Karimov A.A. Algorithmic Method of Organization of Specialized Workshops // International Journal of Advanced Research in Science, Engineering and Technology. 2018. Vol. 5, iss. 4. P. 5670–5675.

6. Normatov I.Kh. Algorithm for detection and neutralization of threats based on functioning tables // IV International Kosygin Forum "Problems of Engineering Sciences: Formation of Technological Sovereignty". Collection of scientific papers of the International Scientific and Technical Symposium "Modern Engineering Problems of Key Branches of the Country's Economy" (February 20–22, 2024). Vol. 1. Moscow: A.N. Kosygin State University, 2024. P. 78–84. (In Russian)

7. Normatov I.Kh., Atazhanov M.N. The effectiveness of using artificial intelligence (AI) in the educational process // International scientific and practical Conference of students, undergraduates, doctoral students and young scientists "Student, science and Innovation: modem research trends" dedicated to the Day of Science workers and the 125th anniversary of Kanysh Satpayev, April 10, 2024. (In Russian)

8. Normatov I., Atazhanov M., Karimov R. Development of an algorithmic system for detecting and disarming threats based on functioning tables // Technical means of information protection: Proceedings of the XXIII International Scientific and Technical Conference, Minsk, April 8, 2025 / Belarusian State University of Informatics and Radioelectronics [et al.]; ed. board: O. V. Boiprav [et al.]. Minsk, 2025. pp. 22–26.

Информация об авторах

Норматов И.Х., доктор физико-математических наук, профессор, директор Научно-инновационного центра «Цифровые технологии и кибербезопасности» имени академика В.К.Кабулова при Национального университета Узбекистана имени Мирзо Улугбека i_normatov@nuu.uz.

Дадажанов Р.Н., кандидат физико-математических наук, доцент Университета общественной безопасности Республики Узбекистан, Ташкент, Узбекистан dadajonovrn@mail.ru.

Атажонов М.Н., преподаватель Военно-академического лицея имени Джалалуддина Мангуберди, muzaffar19910627@gmail.com.

Information about the author

Normatov I.Kh., Doctor of Physical and Mathematical Sciences, Professor, Director of the Scientific and Innovation Center "Digital Technologies and Cybersecurity" named after Academician V.K. Kabulov at the National University of Uzbekistan named after Mirzo Ulugbek, i_normatov@nuu.uz.

Dadazhanov R.N., Candidate of Physical and Mathematical Sciences, Associate Professor, University of Public Security of the Republic of Uzbekistan, Tashkent, Uzbekistan, dadajonovrn@mail.ru.

Atadzhanov M.N., Lecturer, Military Academic Lyceum named after Jalaluddin Manguberdi, muzaffar19910627@gmail.com.