2.Kolmogoroff, A. Zur Theorie der stetigen zuf˙alligen Prozesse // Math. Ann. 1933. Bd. 108, H. 1. S. 149-160.

3.Pollard, J. M. Theorems on factorization and primality testing. // Mathematical Proceedings of the Cambridge Philosophical Society. – 1974. – Vol. 76, no. 3. – P. 521. – doi:10.1017/S0305004100049252.

4.Solovay, Robert M. and Volker Strassen. A fast Monte-Carlo test for primality (англ.) // SIAM Journal on Computing[англ.] : journal. – 1977, submitted in 1974. – Vol. 6, no. 1. – P. 84-85. – doi:10.1137/0206006

5.Lenstra, Jr., H. W. Factoring integers with elliptic curves (англ.) // Annals of Mathematics : journal. – 1987. – Vol. 126, no. 2. – P. 649-673.

6.Shor, P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring (англ.) // Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on – IEEE, 1994. – P. 124-134. – ISBN 0-8186-6580-7 – doi:10.1109/SFCS.1994.365700

7.Bahai, A., Saltzberg, B., Ergen, M. Multi-Carrier Digital Communications: Theory and Publications of OFDM // Springer, New york, 2004.

8.Hanzo, L, Webb, W., Keller, T. Single- and Multi-carrier Quadrature Amplitude Modulation // Wiley, New York, 2000.

Цветов Виктор Петрович, к.физ.-мат.наук, доцент, доцент каф. безопасности информационных систем, tsf-su@mail.ru.

УДК 004.942;004.414.23;004.056.53

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ УСТОЙЧИВОСТИ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ ПРИ ОСУЩЕСТВЛЕНИИ КОМПЬЮТЕРНЫХ АТАК

А. В. Кулдыркаев, В. Е. Дементьев
Мордовский государственный университет имени Н. П. Огарева, г.Саранск

Ключевые слова: математическое моделирование**,** оценка защищенности, облачная инфраструктура, устойчивость инфраструктуры

Одной из важнейших особенностей современных информационных технологий является широкое применение виртуализации и облачных вычислений. Оборотной стороной этих решений является появление новых актуальных угроз безопасности, из-за чего возникает задача оценки устойчивости размещенных в облачной инфраструктуре объектов информатизации при реализации различных сценариев компьютерных атак [1]. Очевидно, что реализация критичных угроз не является единичным событием, а представляет собой многоэтапную последовательность действий злоумышленника.

В настоящей работе для оценки устойчивости размещенных в облачной инфраструктуре объектов предлагается использовать инструменты имитационного моделирования, позволяющие математически прогнозировать исходы компьютерных атак и эффективность средств защиты.

Формализация модели. Вероятность успешной реализации комплексной целевой атаки на компоненты инфраструктуры напрямую зависит от вероятности успешного выполнения злоумышленником последовательности действий $S = \{A_1, A_2, A_i, \dots, A_n\}$, где A_i – i-ое действие злоумышленника, а n – общее количество шагов, необходимых для компрометации целевого компонента инфраструктуры. Для математической формализации введем следующие параметры:

$P(A_i)$ – вероятность реализации i-ной техники. Если считать события независимыми для упрощения первичных расчетов, общая вероятность технического успеха атаки без учета средств защиты составит $P_{\text{общ}} = \prod(i = 1)^n P(A_i)$. t – время, затрачиваемое на реализацию i-го действия. $P(B_i)$ – вероятность обнаружения i-го действия. $\tau_{\text{обн},i}$ – время обнаружения i-го действия. $\tau_{\text{блок}}$ – время блокировки (реакции на инцидент) после его обнаружения.

Каждый шаг атаки описывается вектором $V_i = \{P(A_i), t_i, P(B_i), \tau_{\text{обн},i}\}$. Исходя из введенных параметров, взаимодействие злоумышленника и системы защиты облачной инфраструктуры в рамках сценария S можно свести к трем укрупненным исходам (гипотезам H_1, H_2, H_3):

H_1 – успешная незамеченная атака. Злоумышленник реализует n действий, а система защиты не фиксирует события B_i, либо время обнаружения и реагирования превышает время завершения атаки. Вероятность: $P(H_1) = \prod(i = 1)^n \left[P(A_i) \cdot \left(1 - P_{\text{блок},i}\right)\right]$, где $P_{\text{блок},i}$ – вероятность своевременной блокировки на i-м шаге.

H_2 – успешное реагирование. Система защиты обнаруживает инцидент на шаге k ($1 \leq k \leq n$) и успевает заблокировать доступ. Математическим условием успешного предотвращения атаки, является выполнение временного неравенства $\tau_{\text{обн},k} + \tau_{\text{блок}} < \sum(i = k])^n t_i$. Вероятность сценария:$P(H_2) = 1 - P(H_2) - P(H_3)$;

H_3 – технический провал атаки. Злоумышленник терпит неудачу при реализации одной из техник A_i, независимо от действий системы защиты. Вероятность такого исхода: $P(H_3) = 1 - \prod(i = 1)^n P(A_i)$;

Апробация модели. Для апробации модели рассмотрена усредненная архитектура ЦОД и два сценария атак основанных на методики ФСТЭК России [2] и базе данных MITRE ATT&CK. Сценарий S_1 – отказ в обслуживании на прикладном уровне, состоящий из 3 этапов. Сценарий S_2 – долговременная целевая атака с целью хищения и уничтожения данных, включающий 6 этапов. Программная реализация выполнена на языке программирования Python. Для получения статистически значимых результатов расчет вероятностей гипотез H_1, H_2, H_3 осуществляется методом статистических испытаний с объемом выборки 10000 итераций. В рамках одной итерации алгоритм последовательно моделирует прохождение злоумышленником графа состояний A_i. Для оценки

прикладной значимости модели эксперимент проводился в два этапа:

1. Исходное моделирование для базовой архитектуры.

2. Повторное моделирование после изменения вектора параметров V_i, имитирующего внедрение систем MaxPatrol SIEM (снижение $\tau_{\text{обн},i}$ и рост $P(B_i)$), Kaspersky DDoS Protection (снижение $P(A_i)$ для S_1) и обучения персонала.

Результаты сравнительного имитационного моделирования представлены в таблице 1.

Таблица 1. Сравнение результатов моделирования

Сценарий	**Этап**	H_1, %	H_2, %	H_3, %
S_1	Исходное	76,33	0,22	23,45
	Повторно	7,69	0,17	92,14
S_2	Исходное	3,96	0,27	95,77
	Повторно	1,36	1,08	97,56

Анализ результатов. Для сценария S_1 зафиксировано радикальное снижение вероятности успешной незамеченной атаки H_1 с 76,33 % до 7.69 %. Установка сенсора Kaspersky DDoS Protection привела к провалу атаки на этапе реализации, что также подтверждается увеличением вероятности технического провала H_3 с 23,45 % до 92,14 %.

Также показательной является динамика сценария S_2. Вероятность завершения всего графа атаки H_1 сократилась почти в 3 раза, а вероятность успешного реагирования H_2 возросла в 4 раза. Модель наглядно доказывает, что внедрение системы MaxPatrol SIEM оказывает строго положительное влияние на защищенность инфраструктуры.

В целом, разработанная модель адекватно отражает влияние архитектуры системы безопасности на устойчивость облачной инфраструктуры к таргетированным атакам. Ее применение позволяет математически обосновать требования к допустимому времени обнаружения и блокировки инцидентов, объективно доказать целесообразность внедрения средств защиты информации и расставить приоритеты в дальнейшем развитии защиты инфраструктуры.

Список использованных источников

1.Top Threats to Cloud Computing – Deep Dive 2025 [Электронный ресурс] // Официальный сайт Cloud Security Alliance (CSA). – URL: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2025 (дата обращения: 07.03.2026).

2.Методика оценки угроз безопасности информации от 5 февраля 2021 г. [Электронный ресурс] // Официальный сайт ФСТЭК России. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 07.03.2026).

Кулдыркаев Александр Владимирович, аспирант каф. измерительных и инфокоммуникационных технологий, moran1317@yandex.ru.