МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

На правах рукописи

Миронкин Владимир Олегович

Явные формулы для распределений характеристик итераций случайных отображений

Специальность 05.13.19 — «Методы и системы защиты информации, информационная безопасность»

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва — 2021

Работа выполнена на кафедре математической статистики и случайных процессов механико-математического факультета МГУ имени М.В. Ломоносова.

Научный руководитель — *Зубков Андрей Михайлович*,
доктор физико-математических наук, старший научный сотрудник, заведующий отделом дискретной математики Математического института им. В.А. Стеклова Российской академии наук

Официальные оппоненты — *Харин Юрий Семенович*,
доктор физико-математических наук, член-корреспондент НАН Беларуси, профессор, директор НИИ прикладных проблем математики и информатики Белорусского государственного университета

— *Павлов Юрий Леонидович*,
доктор физико-математических наук, профессор, главный научный сотрудник Института прикладных математических исследований Карельского научного центра РАН

— *Алексеев Евгений Константинович*,
кандидат физико-математических наук, начальник отдела криптографических исследований ООО «КРИПТО-ПРО»

Защита диссертации состоится 24 ноября 2021 г. в 16 часов 45 минут на заседании диссертационного совета МГУ.05.01 ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова» по адресу: 119234, Москва, ГСП-1, Ленинские горы, д. 1, ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», механико-математический факультет, аудитория 14-08.

E-mail: vasenin@msu.ru

С диссертацией можно ознакомиться в отделе диссертаций научной библиотеки МГУ имени М.В. Ломоносова (Ломоносовский просп., д. 27) и на сайте ИАС «ИСТИНА»: https://istina.msu.ru/dissertations/396081864/

Автореферат разослан 20 октября 2021 г.

Ученый секретарь
диссертационного совета МГУ.05.01,
к.ф.-м.н. Кривчиков
Максим Александрович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Развитие раздела теории вероятностей, связанного с исследованием случайных отображений и их модификаций, обусловлено активным применением алгоритмических методов защиты информации (например, конечных автоматов, алгоритмов преобразования данных, алгоритмов хеширования и генерации псевдослучайных последовательностей) (далее — АМЗИ) при решении широкого спектра задач информационной безопасности, а также необходимостью стандартизации отечественных разработок в части, связанной с генерацией производных ключей и псевдослучайных последовательностей. Согласно пп. 17, 18 Доктрины информационной безопасности Российской Федерации, утвержденной Указом президента Российской Федерации № 646 от 5 декабря 2016 года, указанные направления исследований приобретают особую значимость и актуальность.

На сегодняшний день наиболее изученными математическими объектами, используемыми при моделировании АМЗИ и описании режимов их функционирования, являются равновероятные случайные отображения. Однако интенсивное развитие методов синтеза АМЗИ привело к тому, что равновероятные случайные отображения стало невозможно рассматривать как адекватные модели ряда современных АМЗИ, имеющих итерационную структуру. В связи с этим возникла естественная потребность в разработке и обосновании новых теоретико-вероятностных моделей, построенных как на равновероятных, так и на неравновероятных случайных отображениях, с перспективой их дальнейшего использования при создании и исследовании АМЗИ. Примерами подобных неравновероятных отображений являются итерации одного равновероятного случайного отображения и композиции нескольких независимых равновероятных случайных отображений.

Наряду с моделированием процесса работы итерационных АМЗИ, указанные классы отображений могут быть использованы при решении уравнений с однонаправленными функциями, а также при решении целого ряда задач, возникающих в рамках анализа методов балансировки времени-памяти-данных, применяемых для обращения однонаправленных функций и построения радужных таблиц[1].

Степень разработанности темы исследования. Итерации одного и композиция нескольких случайных отображений представляют собой обобщение случайных отображений — математических объектов, широко используемых при решении задач информационной безопасности, и подробно изученных видными российскими и зарубежными учеными,

[1] Пильщиков Д. В., “Исследование сложности метода радужных таблиц с маркерами цепочек”, *Математические вопросы криптографии*, **8**:4 (2017), 99-116.

в частности, В. Н. Сачковым, Б. А. Севастьяновым, В. Е. Степановым, В. Ф. Колчиным, А. М. Зубковым, В. Г. Михайловым, В. Г. Проскуриным, А.Л. Якымивым, А. Одлыжко (A. Odlyzko), Ф. Флажоле (P. Flajolet), Д. Олдосом (D. Aldous), Д. Питманом (J. Pitman), Х. Рубином (H. Rubin), Б. Харрисом (B. Harris), Р. Ситгрейвесом (R. Sitgreaves) и др.

В работах указанных специалистов получен целый спектр результатов, описывающих особенности строения графа случайного отображения, выписаны асимптотические и точные выражения для его характеристик, в том числе подробно изучена цикловая структура как самого отображения, так и ряда производных конструкций, построенных на его основе (автоматные отображения, регистры сдвига и т.д.).

В частности, в работе Х. Рубина и Р. Ситгрейвеса[2], опубликованной в 1954 году, для множества всех n^n отображений $\Omega = \{f\colon S \to S\}$ с заданным на нем равновероятным распределением, где S — произвольное конечное множество, $|S| = n$, $n \in \mathbb{N}$, получены точные выражения для локальных вероятностей общего числа N_f циклических вершин, размера C_f случайной компоненты связности и общего числа M_f компонент связности в графе равновероятного случайного отображения f (далее — G_f):

$$\mathbf{P}\{N_f = j\} = \frac{(n-1)!j}{(n-j)!n^j},$$

$$\mathbf{P}\{C_f = j\} = \frac{(n-1)!}{(n-j)!\,(j-1)!}\frac{j^j\,(n-j)^{n-j}}{n^n}\sum_{i=1}^{j}\frac{(j-1)!}{(j-i)!j^i},$$

$$\mathbf{P}\{M_f = j\} = \sum_{i=1}^{n}\frac{(n-1)!j}{(n-j)!n^j}\alpha\{i,j\},$$

где $j \in \{1,\ldots,n\}$, а $\alpha\{i,j\}$ — коэффициент при z^i в разложении $\frac{\Gamma(z+j)}{\Gamma(z)j!}$ в степенной ряд. Позднее В. Ф. Колчин выписал и асимптотические формулы[3] для этих распределений.

При тех же условиях в работе Б. Харриса[4] для длины $\tau_f(x)$ отрезка апериодичности произвольной фиксированной вершины $x \in S$ и длины $\beta_f(x)$ цикла компоненты связности графа G_f, содержащей x, получены совместные и маргинальные распределения

$$\mathbf{P}\{\tau_f(x) = k, \beta_f(x) = j\} = \frac{(n-1)!}{(n-k)!n^k}, \quad 1 \leqslant j \leqslant k \leqslant n,$$

---

[2] Rubin H., Sitgreaves R., *Probability distributions related to random trans-formations of a finite set*, Tech. Rept. № 19A, Applied Mathematics and Statistics Laboratory, Stanford University, 1954, 50 pp.

[3] Колчин В. Ф., *Случайные графы (2-е изд.)*, М.: ФИЗМАТЛИТ, 2004, 256 с.

[4] Harris B., "Probability distributions related to random mapping", *Ann. Math. Statist.*, 1960, **31**:4 (1960), 1045-1062.

$$\mathbf{P}\{\beta_f(x) = j\} = \sum_{k=j}^{n} \frac{(n-1)!}{(n-k)!n^k}, \quad j \in \{1, 2, \ldots, n\},$$

$$\mathbf{P}\{\tau_f(x) = k\} = \frac{(n-1)!k}{(n-k)!n^k}, \quad k \in \{1, 2, \ldots, n\}.$$

В представленной на международной конференции «Workshop on the Theory and Application of Cryptographic Techniques» (Бельгия, апрель 1989 г.) работе[5] выписана асимптотика при $n \to \infty$ для средних значений случайных величин N_f, M_f, $|T_f|$ и $|f(S)|$, где T_f — множество вершин в графе G_f, не имеющих прообразов, а $f(S)$ — образ множества S при действии случайного отображения f:

$$\mathbf{E}N_f \sim \sqrt{\frac{\pi n}{2}}, \quad \mathbf{E}M_f \sim \frac{\ln n}{2}, \quad \mathbf{E}|T_f| \sim e^{-1}n, \quad \mathbf{E}|f(S)| \sim \left(1 - e^{-1}\right) n.$$

В том числе для композиции независимых равновероятных случайных отображений $f_1, \ldots, f_k$ множества S в себя, где $k \in \mathbb{N}$ — произвольное, авторами получено асимптотическое равенство при $n \to \infty$, $k = const > 0$ для среднего значения случайной величины $|f_k(\ldots(f_1(x))\ldots)(S)|$:

$$\mathbf{E}|f_k(\ldots(f_1(x))\ldots)(S)| \sim (1 - \tau_k)\, n,$$

где $\tau_0 = 0$, $\tau_{k+1} = e^{-1+\tau_k}$.

В 1989 году Л. Мутафчиев[6] для распределения случайной величины, равной мощности t-го слоя $H_f^{(t)} = \{x \in S \colon \alpha_f(x) = t\}$ в графе G_f, для случая $t = o(\sqrt{n})$ при $n \to \infty$ доказал сходимость к распределению Рэлея с модой 1 при $n \to \infty$:

$$\mathbf{P}\left\{\frac{\left|H_f^{(t)}\right|}{\sqrt{n}} \leqslant z\right\} \to 1 - e^{-\frac{z^2}{2}}, \quad z \geqslant 0,$$

позволившую получить асимптотики для численных характеристик случайной величины $\left|H_f^{(t)}\right|$ при $n \to \infty$ в области типичных значений:

$$\mathbf{E}\left|H_f^{(t)}\right| \sim \sqrt{\frac{\pi n}{2}} \quad \text{и} \quad \mathbf{D}\left|H_f^{(t)}\right| \sim \left(2 - \frac{\pi}{2}\right) n.$$

Позднее указанный результат был обобщен в статье М. Дрмота и М. Сория[7] для произ-

[5] Flajolet P., Odlyzko A., "Random Mapping Statistics", *Lect. Notes Comput. Sci. 434*, EUROCRYPT'89, 1989, 329-354.

[6] Mutafchiev L., "The limit distribution of the number of nodes in low strata of a random mapping", *Statist. Probab. Lett.*, **7** (1989), 247-251.

[7] Drmota M., Soria M., "Images and preimages in a random mapping", *SIAM Journal on Discrete Mathematics*,

вольного $t > 0$. В этой же статье для числа $\nu_f(r)$ вершин кратности r (т.е. вершин в графе G_f, имеющих в точности r прообразов) доказана локальная сходимость при $n \to \infty$ к стандартному нормальному закону для произвольного фиксированного $r \geqslant 0$:

$$\mathbf{P}\left\{\frac{\nu_f(r) - n\mu_r}{\sigma_r\sqrt{n}} \leqslant x\right\} \to \Phi(x),$$

где $\mu_r = \frac{1}{er!}$, $\sigma_r^2 = \mu_r + \left(1 + (r-1)^2\right)\mu_r^2$, а в работе[8] этот результат обобщен на случай отличного от константы функционала $r = r(n)$. Так, в частности, в случае $r(n) \sim \lambda n^{\frac{2}{3}}$, где $\lambda > 0$, при $n \to \infty$ распределение случайной величины $\nu_f(r)$ сходится к пуассоновскому распределению $\Pi(\lambda)$, а в случае $r(n) = o(n)$ при $n \to \infty$ — к стандартному нормальному распределению $\mathcal{N}(0,1)$.

На X Всероссийском симпозиуме по прикладной и промышленной математике (Санкт-Петербург, май 2009 г.) в рамках доклада А. М. Зубкова и П. В. Халипова «Вероятность попадания нескольких точек в одну компоненту связности случайного отображения», посвященного исследованию строения компонент связности графа G_f, для произвольных вершин $x_1, \ldots, x_k \in S$, где $k \geqslant 2$, сформулирован следующий результат:

$$\lim_{n\to\infty} \mathbf{P}\{x_1, \ldots, x_k \in \mathcal{K}_f(x_1)\} = \frac{(2k-2)!!}{(2k-1)!!},$$

где $\mathcal{K}_f(x_1)$ — компонента связности графа G_f, содержащая вершину x_1.

Отдельную группу формируют результаты исследований различного рода модификаций равновероятных случайных отображений. Так, использование кратных итераций равновероятного случайного отображения позволило оптимизировать двухэтапный метод М. Хеллмана[9] решения уравнений вида $g(x) = a$, где $g\colon S \to S$ — произвольная однонаправленная функция[10], а $|S| = n$. В частности, Д. В. Пильщиковым[11] получены оценки временной сложности оперативного этапа метода Хеллмана с использованием радужных таблиц и маркеров цепочек, а также рассчитана средняя временная сложность полной обработки одной такой таблицы.

В свою очередь, в статье А. М. Зубкова и А. А. Серова[12] изучалась модель построения

---

10 (1996), 246-269.

[8] Baron G., Drmota M., Mutafchiev L., "Predecessors in Random Mappings", *Combinatorics, Probability and Computing*, **5** (1996), 317-335.

[9] Hellman M. E., "A cryptanalytic time-memory trade-off", *IEEE Trans. Inf. Theory*, 1980, 401-406.

[10] Погорелов Б. А., Сачков В. Н., *Словарь криптографических терминов*, М.: МЦНМО, 2006, 94 с.

[11] Пильщиков Д. В., "Исследование сложности метода радужных таблиц с маркерами цепочек", *Математические вопросы криптографии*, **8**:4 (2017), 99-116.

[12] Зубков А. М., Серов А. А., "Совокупность образов подмножества конечного множества при итерациях

радужной таблицы на основе композиции независимых равновероятных случайных отображений $f_1, \ldots, f_k$ множества S в себя, где $k \in \mathbb{N}$. Для произвольного $S_0 \subseteq S$, $|S_0| = m \leqslant n$ и соответствующих последовательностей множеств

$$S_k = f_k\left(f_{k-1}\left(\ldots\left(f_1\left(S_0\right)\right)\ldots\right)\right), \quad \Psi_k = S_1 \cup \ldots \cup S_k, \quad k = 1, 2, \ldots,$$

описан способ точного вычисления распределений случайных величин $\varphi_k = |S_k|$ и $\zeta_k = |\Psi_k|$ с использованием аппарата цепей Маркова. В том числе получены верхние и нижние оценки для некоторых условных характеристик:

$$\frac{m}{n} - C_m^2\frac{k}{n^2} \leqslant \mathbf{P}\{x \in S_k \mid \varphi_0 = m\} < \frac{m}{n} - C_m^2\frac{k}{n^2} + \frac{m^3k^2}{4n^3},$$

$$\frac{mk}{n} - C_{k+1}^2\frac{3m^2}{2n^2} < \mathbf{P}\{x \in \Psi_k \mid \varphi_0 = m\} < \frac{mk}{n} - C_m^2C_{k+1}^2\frac{1}{n^2} + \frac{m^3\left(k+1\right)^3}{12n^3},$$

$$m - C_m^2\frac{k}{n} \leqslant \mathbf{E}\{\varphi_k \mid \varphi_0 = m\} < n - C_m^2\frac{k}{n} + \frac{m^3k^2}{4n^2},$$

$$mk - C_{k+1}^2\frac{3m^2}{2n} < \mathbf{E}\{\zeta_k \mid \varphi_0 = m\} < mk - C_m^2C_{k+1}^2\frac{1}{n} + \frac{m^3\left(k+1\right)^3}{12n^2},$$

$$\mathbf{D}\{\varphi_k \mid \varphi_0 = m\} < \frac{km^3}{n}\left(1 + \frac{\left(m+2\right)k}{4mn}\right).$$

Этими же авторами[13] доказана асимптотическая нормальность случайной величины φ_k при $l, m, k, n \to \infty : l = O\left(n^{\frac{1}{4}}\right)$, $m = o\left(l\right)$, $k = 2n\left(\frac{1}{m} - \frac{1}{l}\right) + \left(1 + o\left(1\right)\right)x\frac{2n}{\sqrt{3}}\sqrt{\frac{1}{m^3} - \frac{1}{l^3}}$, где $x \in \mathbb{R}$:

$$\mathbf{P}\left\{\varphi_k \leqslant \frac{n}{n/l + k/2}\right\} \to \Phi\left(x\right),$$

а также выписаны точные формулы для следующих условных распределений:

$$\mathbf{P}\{\varphi_k = m \mid \varphi_0 = m\} = \prod_{i=1}^{m-1}\left(1 - \frac{i}{n}\right)^k,$$

$$\mathbf{P}\{\varphi_k = m-1 \mid \varphi_0 = m\} = \frac{m}{2}\left(1 - \left(1 - \frac{m-1}{n}\right)^k\right)\prod_{i=1}^{m-2}\left(1 - \frac{i}{n}\right)^k,$$

$$\mathbf{P}\{\varphi_k = m-a \mid \varphi_{k-1} = m\} = \sum_{2 \leqslant j_1 < j_2 < \ldots < j_a \leqslant m}\prod_{i=1}^{m-a-1}\left(1 - \frac{i}{n}\right)\prod_{v=1}^{a}\frac{j_v - v}{n}.$$

случайных отображений", *Дискретная математика*, **26**:4 (2014), 43-50.

[13] Зубков А. М., Серов А. А., "Предельная теорема для мощности образа подмножества при композиции случайных отображений", *Дискретная математика*, **29**:1 (2017), 17-26.

В работе[14] получены двусторонние неравенства для $\mathbf{E}\{\varphi_k \mid \varphi_0 = m\}$, в которых разность между верхней и нижней оценками имеет порядок $o(m)$ при $m, k, n \to \infty$: $mk = o(n)$.

Задачи, связанные с оценкой скорости сжатия исходного множества S при действии композиции отображений и имеющие особое практическое значение при моделировании алгоритмов выработки производных ключей, решались в работе А. М. Зубкова и О. К. Шибанова[15]. Так, в частности, для

$$\tau_n = \min\{t \in \mathbb{N}\colon |f_t(\ldots(f_1(S))\ldots)| = 1\},$$

где $f_1, \ldots, f_k$ — независимые равновероятные случайные отображения множества S в себя, доказана сходимость распределения случайной величины $\zeta = \frac{1}{n}\tau_n$ при $n \to \infty$ к распределению суммы $\xi = \sum\limits_{j=1}^{\infty} \xi_j$, где случайные величины $\xi_1, \xi_2, \ldots$ независимы и

$$\mathbf{P}\{\xi_j \leqslant x\} = 1 - e^{-xC_{j+1}^2}, \quad x \geqslant 0, \quad j = 1, 2, \ldots,$$

а для случайной величины ξ выполняется равенство

$$\mathbf{E}\xi = \sum_{j=1}^{\infty} \frac{2}{j(j+1)} = 2.$$

Другая модификация итераций отображений, построенная на основе одного равновероятного случайного отображения $f\colon S \to S$ и последовательности $R_1, R_2, \ldots$ случайных независимых биективных отображений множества S в себя, изучалась в статье Ф. Очслина[16]. Так, для подмножества $S_0 \subset S$, $|S_0| = m$, и последовательности его образов

$$S_k = R_k(f(\ldots(R_1(f(S_0)))\ldots)), \quad k = 1, 2, \ldots,$$

и случайного множества

$$\widetilde{\Psi}_k = S_1 \cup \ldots \cup S_k, \quad k = 1, 2, \ldots,$$

[14]Зубков А. М., Серов А. А., "Оценки среднего размера образа подмножества при композиции случайных отображений", *Дискретная математика*, **30**:2 (2018), 27-36.

[15]Зубков А. М., Шибанов О. К., "Время до объединения всех частиц при равновероятных размещениях по последовательности слоев ячеек", *Матем. заметки*, **85**:3 (2009), 373-381

[16]Oechslin P., "Making a faster cryptanalytic time-memory trade-off", *Lect. Notes Comput. Sci.*, **2729** (2003), 617-630.

с использованием эвристических рассуждений получена приближенная формула

$$\mathbf{P}\{x \in S_0 \cup \widetilde{\Psi}_k\} \approx 1 - \prod_{i=1}^{k} \left(1 - \frac{n_i}{n}\right),$$

где $n_1 = m,\ n_{i+1} = n\left(1 - e^{-\frac{n_i}{n}}\right)$ при $i \geqslant 1$.

В свою очередь, для случайного множества

$$\Phi_k = f(S_0) \cup f^2(S_0) \cup \ldots \cup f^k(S_0)$$

в 1980 году М. Хеллманом[9] была получена двусторонняя оценка

$$\frac{1}{n}\sum_{i=1}^{m}\sum_{j=1}^{k}\left(1 - \frac{ik}{n}\right)^j \leqslant \mathbf{P}\{x \in \Phi_k\} \leqslant \frac{mk}{n},$$

справедливая для произвольного $x \in S$. В частности, автор показал, что при $mk^2 \approx n$ и $m, k \geqslant 1$ левая часть этого неравенства близка к $0,80\frac{mk}{n}$. Позднее К. Кусуда и Т. Матсумото[17] вывели более точную нижнюю оценку

$$\frac{1}{n}\sum_{i=1}^{m}\sum_{j=1}^{k}\left(1 - \frac{ik}{n}\right)^j \geqslant \frac{mk}{n}\int_0^1 \frac{1 - e^{-x}}{x} kx \approx 0,796599\frac{mk}{n},$$

а с помощью перехода к аппроксимирующим дифференциальным уравнениям[18] — приближенную формулу:

$$\mathbf{P}\{x \in \Phi_k\} \approx 2\left(1 - \frac{1}{\tau^2}\right)\frac{e^{\frac{k}{\tau}} - e^{-\frac{k}{\tau}}}{(\tau+1)e^{\frac{k}{\tau}} + (\tau-1)e^{-\frac{k}{\tau}}},$$

где $\tau = \sqrt{\frac{2n}{m}}$.

Наконец, в статье А. А. Серова[19] изучались последовательности независимых пар зависимых равновероятных случайных отображений (f_1, g_1), $(f_2, g_2), \ldots$ множества S в себя, удовлетворяющих условиям

$$\mathbf{P}\{f_k(x) = g_k(x) = y\} = \frac{\alpha}{n},$$

---

[17] Kusuda K., Matsumoto T., "Optimization of time-memory trade-off crypta-nalysis and its application to DES, FEAL-32, and Skipjack", *IEICE Trans. on Fundamentals*, **1**:E-79A (1996), 35-48.

[18] Hong J., Ma D., "Success probability of the Hellman trade-off", *Inf. Process. Lett.*, **109**:7 (2009), 347-351.

[19] Серов А. А., "Образы конечного множества при итерациях двух случайных зависимых отображений", *Дискретная математика*, **27**:4 (2015), 133-140.

$$\mathbf{P}\{f_k(x) = y, g_k(x) = z\} = \frac{1-\alpha}{n(n-1)}$$

для любых $y, z \in S$, $y \neq z$, где $\frac{1}{n} \leqslant \alpha < 1$. Так, для множеств

$$S_k = f_k(\ldots(f_1(S_0))\ldots), \quad T_k = g_k(\ldots(g_1(S_0))\ldots)$$

при любых $1 \leqslant k,\ m \leqslant n$ и произвольном фиксированном $x \in S$ автором выписаны двусторонние оценки

$$L(k,n) \leqslant \mathbf{P}\{x \in S_k \cap T_k \mid |S_0| = m\} < L(k,n) + U(k,n),$$

где при $\lambda_1 = 1 - \frac{1}{n},\ \lambda_2 = \alpha - \frac{1}{n},\ \lambda_3 = \left(1 - \frac{2}{n}\right)\left(\alpha - \frac{1}{n}\right)$

$$L(k,n) = \frac{m}{n}\frac{1 + n(1-\alpha)(2-\lambda_2^t)}{n(1-\lambda_2)} - \frac{m(m-1)}{n}\left(1 - \lambda_1^t + \frac{1-\lambda_2^t}{n(1-\lambda_2)}\right),$$

$$U(k,n) = \frac{m(m-1)}{n^2}\left(\frac{(m-2)k^2}{2n} + \frac{m\left(1-\lambda_1^k\right)}{1-\lambda_2}\right) + \\ + \frac{m(m-1)}{n^2}\left(\frac{\lambda_2\left(\lambda_1^k m - \lambda_3^k(m-2)\right)}{(n(1-\alpha)+2\lambda_2)(1-\lambda_2)} + \frac{n\left(\lambda_2^k - \lambda_3^k\right)(1-\alpha)}{1-\lambda_2}\right).$$

Цель исследования. Построение и исследование адекватных математических моделей современных итерационных АМЗИ, основанных на итерациях одного или нескольких независимых равновероятных случайных отображений конечного множества в себя, с перспективой их дальнейшего использования при создании новых и совершенствовании действующих АМЗИ.

Задачи исследования.

- Исследование структуры графа G_{f^k}, где f^k — k-кратная итерация равновероятного случайного отображения $f\colon S \to S$, в том числе множеств циклических, висячих вершин, прообразов произвольных вершин, слоев и образа $f^k(S)$, $k \in \mathbb{N}$.

  Вывод точных выражений и неравенств для вероятностей инцидентности вершин перечисленным выше множествам, вероятностей коллизий, а также для распределений основных характеристик графа G_{f^k}: длин отрезков апериодичности, подходов, циклов и т. д.

- Исследование структуры графа $G_{f_{[k]}}$, где $f_{[k]}$ — композиция k независимых равнове-

роятных случайных отображений $f_i\colon S \to S$, $i = 1, \ldots, k$, в том числе множеств циклических, висячих вершин, прообразов произвольных вершин, слоев и образа $f_{[k]}(S)$, $k \in \mathbb{N}$.

Вывод точных выражений и неравенств для вероятностей инцидентности вершин перечисленным выше множествам, вероятностей коллизий, а также для распределений основных характеристик графа $G_{f_{[k]}}$: длин отрезков апериодичности, подходов, циклов и т. д.

Положения, выносимые на защиту. На защиту выносятся: обоснование актуальности, научная новизна, теоретическая и практическая значимость работы, а также следующие положения, которые подтверждаются результатами исследования, представленными в Заключении диссертации.

1. Для графа k-кратной итерации равновероятного случайного отображения конечного множества S в себя, $k \in \mathbb{N}$:

   а) формулы и неравенства для распределений длины отрезка апериодичности и высоты произвольной фиксированной вершины (§ 1.2, § 1.4);

   б) формулы и неравенства для вероятностей инцидентности вершин множеству циклических вершин и одной компоненте связности (§ 1.4, § 1.5);

   в) формулы для вероятностей инцидентности вершин слоям и множеству прообразов произвольной фиксированной вершины (§ 1.4, § 1.6);

   г) формула для вероятности появления коллизии (§ 1.6).

2. Для графа композиции k независимых равновероятных случайных отображений конечного множества S в себя, $k \in \mathbb{N}$:

   а) точные, предельные формулы, а также неравенства для распределений длины отрезка апериодичности и высоты произвольной фиксированной вершины (§ 2.2);

   б) формулы и неравенства для вероятностей инцидентности вершин слоям и множеству циклических вершин (§ 2.3);

   в) формулы для вероятностей появления коллизии и инцидентности вершин образу исходного множества вершин (§ 2.4);

   г) формулы для вероятностей инцидентности вершин одной компоненте связности и множеству прообразов произвольной фиксированной вершины (§ 2.5, § 2.6).

Научная новизна. Построены новые математические модели, основанные на неравновероятных случайных отображениях: кратной итерации равновероятного случайного отображения конечного множества в себя и композиции нескольких независимых случайных отображений конечного множества в себя, позволяющие адекватно описывать современные итерационные АМЗИ. Получены явные формулы для распределений вероятностных характеристик указанных моделей.

Теоретическая значимость. Полученные в диссертации явные формулы для распределений вероятностных характеристик моделей, основанных на кратной итерации равновероятного случайного отображения конечного множества в себя и композиции нескольких независимых случайных отображений конечного множества в себя, могут быть использованы при синтезе и анализе современных итерационных АМЗИ, предназначенных для преобразования и хеширования данных, выработки производных ключей и генерации псевдослучайных последовательностей, а также при обосновании их теоретической стойкости.

Практическая значимость. Полученные в диссертации явные формулы для распределений вероятностных характеристик моделей, основанных на кратной итерации равновероятного случайного отображения конечного множества в себя и композиции нескольких независимых случайных отображений конечного множества в себя, находят свое применение при обосновании выбора параметров итерационных АМЗИ, используемых при выработке производных ключей, существенно влияющих на безопасность обрабатываемой с их использованием информации.

Практическая значимость диссертации подтверждена двумя актами о внедрении. Результаты диссертации использованы в деятельности ПФ ФГУП «НТЦ «Атлас» в рамках сертификационных исследований создаваемых средств защиты информации, а также в деятельности ООО «КРИПТО-ПРО» при выборе параметров, ограничивающих количество преобразований одного ключа с использованием механизма «CryptoPro Key Meshing».

Результаты первой главы учтены при синтезе и анализе усовершенствованного механизма периодической смены ключа ACPKM, вошедшего в документ Росстандарта Р 1323565.1.017-2018 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования» и используемого в настоящее время в продуктах компаний-разработчиков средств защиты информации в качестве одного из основных методов защиты информации в части преобразования ключей.

Методология и методы исследования. Настоящие исследования базируются на известных теоретических положениях дискретной математики, теории вероятностей, теории графов, математического и комбинаторного анализа.

Достоверность результатов исследования. Достоверность полученных результатов обеспечивается строгими математическими доказательствами утверждений и подтверждается их согласованностью с данными, полученными в ходе вычислительных экспериментов.

Результаты других авторов, упомянутые в тексте диссертации, отмечены соответствующими ссылками.

Соответствие диссертации паспорту научной специальности. Содержание диссертации соответствует паспорту специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность» в части п. 1 «Теория и методология обеспечения информационной безопасности и защиты информации», п. 9 «Модели и методы оценки защищенности информации и информационной безопасности объекта» и п. 13 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

Апробация результатов исследования. Результаты диссертации доложены на следующих семинарах, всероссийских конференциях и симпозиумах:

1. XV Всероссийский Симпозиум по прикладной и промышленной математике (весенняя сессия) (Кисловодск, 1 мая — 8 мая 2014 г.).

2. XVII научно-практическая конференция «РусКрипто'2015» (Московская область, Солнечногорский район, 17 марта — 20 марта 2015 г.).

3. Научный семинар «Математические методы криптографического анализа» МГУ имени М.В. Ломоносова (Москва, 6 апреля 2015 г.).

4. XVI Всероссийский Симпозиум по прикладной и промышленной математике (летняя сессия) (Челябинск, 21 июня — 27 июня 2015 г.).

5. XVI Всероссийский Симпозиум по прикладной и промышленной математике (осенняя сессия)[20] (Сочи, 27 сентября — 4 октября 2015 г.).

[20]Доклад отмечен медалью и грамотой за III место в III Общероссийском открытом конкурсе «Отмеченная работа молодого исследователя в области прикладной и промышленной математики» в 2015 году.

6. XVII Всероссийский Симпозиум по прикладной и промышленной математике (весенняя сессия) (Кисловодск, 1 мая — 8 мая 2016 г.).

Публикации по теме исследования. По теме диссертации опубликовано 8 статей в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность» и входящих в списки Scopus или RSCI WoS.

Структура и объём диссертации. Диссертация состоит из введения, двух глав, разделенных на параграфы, заключения, списка сокращений и условных обозначений, а также списка литературы, включающего 84 наименования. Текст диссертации изложен на 134 страницах с 8 рисунками.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во Введении обоснованы актуальность темы диссертации и степень ее разработанности, сформулированы цели и задачи, решаемые в рамках настоящего исследования. Представлены положения, выносимые на защиту. Описаны научная новизна, теоретическая и практическая значимость результатов диссертации.

В первой главе диссертации исследована структура графа k-кратной итерации одного равновероятного случайного отображения конечного множества в себя, $k \in \mathbb{N}$. В частности, для множества $S = \{1, \ldots, n\}$, $n > 1$, и вероятностного пространства $(\Omega, \mathcal{F}, \mathbf{P})$, в котором пространством элементарных исходов Ω является множество $\mathfrak{S}$ всех n^n отображений $f\colon S \to S$, алгеброй событий $\mathcal{F}$ — множество всех подмножеств Ω, а вероятностная мера $\mathbf{P}$, соответствующая равновероятным случайным отображениям, задана следующим образом:

$$\mathbf{P}(f) = \frac{1}{n^n} \quad \forall\, f \in \Omega, \tag{1}$$

получен ряд результатов, описывающих теоретико-вероятностные свойства и характеристики графа G_{f^k}, которые могут быть использованы при моделировании и исследовании итерационных АМЗИ типа «CryptoPro Key Meshing»[21].

Замечание. Нумерация приведенных ниже теорем и следствий, выносимых на защиту, в точности соответствует нумерации результатов в диссертации.

[21] Миронкин В. О., "О некоторых вероятностных характеристиках алгоритма выработки ключа «CRYPTOPRO KEY MESHING»", *Проблемы информационной безопасности. Компьютерные системы*, 2015, № 4,140-146.

При изложении основных результатов диссертации будем использовать следующие стандартные обозначения: $]z[= \min\{n \in \mathbb{Z}\colon n \geqslant z\}$, $[z] = \max\{n \in \mathbb{Z}\colon n \leqslant z\}$, а $(n)_k = n(n-1)\ldots(n-k+1)$ — k-я факториальная степень числа n.

Дополнительно для произвольных $i = 1, 2$ и $k, l, j \in \mathbb{N}$, $j \geqslant i$, обозначим

$$Q_i^j(k,l) = \{m \in \mathbb{N}\colon i \leqslant m \leqslant j,\ \frac{m}{(m,k)} = l\}, \tag{2}$$

$$\tilde{Q}_i^j(k,l) = \{m \in \mathbb{N}\colon i \leqslant m \leqslant j,\ \frac{m}{(m,k)} < l\}, \tag{3}$$

а для любых $i_0, i_1 \in \mathbb{Z}\colon i_0 > i_1$ положим $\sum\limits_{j=i_0}^{i_1}(\ldots) \equiv 0$, $\prod\limits_{j=i_0}^{i_1}(\ldots) \equiv 1$.

Для длины $\tau_{f^k}(x)$ отрезка апериодичности, начинающегося в вершине $x \in S$ графа G_{f^k}, доказан следующий результат.

Теорема 1.1. *Пусть случайное отображение $f\colon S \to S$ имеет распределение (1) на Ω. Тогда для любого фиксированного $x \in S$ и любых $k \in \mathbb{N}$, $z \in \{1, \ldots, n\}$ справедливо равенство*

$$\mathbf{P}\left\{\tau_{f^k}(x) = z\right\} = \sum_{m \in Q_1^n(k,z)} \frac{(n)_m}{n^{m+1}} + \sum_{m \in \tilde{Q}_1^n(k,z)} \sum_{v=1}^{\min(k,n-r)} \frac{(n)_{r+v}}{n^{r+v+1}},$$

где $r = m + \left(z - \frac{m}{(m,k)} - 1\right)k$, а $Q_1^n(k,z)$ и $\tilde{Q}_1^n(k,z)$ определяются соотношениями (2), (3).

Через F_k обозначим функцию распределения случайной величины $\tau_{f^k}(x)$ для произвольной фиксированной вершины $x \in S$ (в силу равноправия вершин из S зависимость от x отражать не будем).

Теорема 1.2. *Пусть случайное отображение $f\colon S \to S$ имеет распределение (1) на Ω. Тогда для любого фиксированного $x \in S$ и любых $k \in \mathbb{N}$, $z \in \{1, \ldots, n\}$, $kz \leqslant n$, справедливы равенства*

$$F_k(z) = \sum_{m \in \tilde{Q}_1^n(k,z+1)} \sum_{t=0}^{\left(z - \frac{m}{(m,k)}\right)k} \frac{(n)_{m+t}}{n^{m+t+1}}$$

и

$$F_k(z) = \frac{1}{n} \sum_{u=1}^{k} \sum_{j=0}^{\left[\frac{(k,u)z-u}{k}\right]} S\left(kj+u, \left(z - \frac{kj+u}{(u,k)}\right)k\right),$$

где $S(m,W) = \sum\limits_{t=0}^{W} \frac{(n)_{m+t}}{n^{m+t}}$, а $\tilde{Q}_1^n(k,z)$ определяется соотношением (3).

Теорема 1.4. *Пусть случайное отображение $f\colon S \to S$ имеет распределение (1) на Ω. Тогда для любого фиксированного $x \in S$ и любого $k \in \mathbb{N}$ справедливо равенство*

$$\mathbf{P}\left\{x \in f^k(S)\right\} = \sum_{l=1}^{n} \frac{(n)_l}{n^{l+1}} + \sum_{t=1}^{n-1} \sum_{l=t+1}^{n} \frac{(n-1)_{l-1}}{n^l} \sum_{m=1}^{n-l} (-1)^{m-1} B_{n-l,m}^{(k)},$$

где величины $B_{n-l,m}^{(k)}$ удовлетворяют равенствам

$$B_{n-l,m}^{(1)} = \frac{C_{n-l}^{m}}{n^m}, \quad B_{n-l,m}^{(k)} = \sum_{s=1}^{m} a_{n-l,m,s} B_{n-l-m,s}^{(k-1)}, \ k \geqslant 2,$$

а числа $a_{n-l,m,s}$ определяются соотношением

$$a_{n-l,m,s} = C_{n-l-m}^{s} \left(\frac{s}{n}\right)^m \sum_{t=0}^{s} C_s^t (-1)^t \left(1 - \frac{t}{s}\right)^m.$$

Через T_{f^k} обозначим множество висячих (т.е. не имеющих прообразов) вершин в графе G_{f^k}.

Следствие 1.4. *Пусть случайное отображение $f\colon S \to S$ имеет распределение (1) на Ω. Тогда для любого фиксированного $x \in S$ и любого $k \in \mathbb{N}$ справедливо равенство*

$$\mathbf{P}\{x \in T_{f^k}\} = 1 - \sum_{l=1}^{n} \frac{(n)_l}{n^{l+1}} - \sum_{t=1}^{n-1} \sum_{l=t+1}^{n} \frac{(n-1)_{l-1}}{n^l} \sum_{m=1}^{n-l} (-1)^{m-1} B_{n-l,m}^{(k)}.$$

Через $C_l(G_{f^k})$ обозначим множество циклических вершин графа G_{f^k}, лежащих на циклах длины $l \in \{1, \ldots, n\}$.

Теорема 1.5. *Пусть случайное отображение $f\colon S \to S$ имеет распределение (1) на Ω. Тогда для любого фиксированного $x \in S$ и любого $k \in \mathbb{N}$, $l \in \{1, \ldots, n\}$ справедливо равенство*

$$\mathbf{P}\left\{x \in C_l\left(G_{f^k}\right)\right\} = \sum_{m \in Q_1^n(k,l)} \frac{(n)_m}{n^{m+1}},$$

где $Q_1^n(k,l)$ определяется соотношением (2).

Для произвольных $l \in \{1, \ldots, n\}$, $t \in \{0, \ldots, n-l\}$ определим множество вершин $H_{f^k}^{(t,l)} = \left\{x \in S\colon \alpha_{f^k}(x) = t, \beta_{f^k}(x) = l\right\}$.

Теорема 1.7. *Пусть случайное отображение $f\colon S \to S$ имеет распределение (1) на Ω. Тогда для любого фиксированного $x \in S$ и любых $k \in \mathbb{N}$, $l \in \{1, \ldots, n\}$ и $t \in \{1, \ldots, n-l\}$*

справедливо равенство

$$\mathbf{P}\left\{x \in H_{f^k}^{(t,l)}\right\} = \sum_{s=0}^{k-1} \sum_{m \in Q_1^{n-tk+s}(k,l)} \frac{(n)_{m+tk-s}}{n^{m+tk-s+1}},$$

где $Q_1^n(k,l)$ *определяется соотношением* (2).

Для произвольного фиксированного $x \in S$ через $\mathcal{K}_{f^k}(x)$ обозначим компоненту связности графа G_{f^k}, содержащую x.

Теорема 1.10. *Пусть случайное отображение* $f\colon S \to S$ *имеет распределение* (1) *на* Ω. *Тогда для любых фиксированных* $x, y \in S$, $x \neq y$, *и любого* $k \in \mathbb{N}$ *справедливо равенство*

$$\mathbf{P}\left\{y \in \mathcal{K}_{f^k}(x)\right\} = \sum_{m=1}^{n} \sum_{v=m}^{n} \sum_{s=0}^{n-v} \frac{\left(\left]\frac{v}{(m,k)}\right[- \omega_{m,v,s}\right)(n-2)_{v+s-2}}{n^{v+s}},$$

где $\omega_{m,v,s} = \begin{cases} 1, & \text{если } s = 0, \\ \Delta_{(m,k)}^{s,v} & \text{в противном случае,} \end{cases}$ *а* $\Delta_{(m,k)}^{s,v}$ *определяется соотношением*

$$\Delta_{(m,k)}^{s,v} = \begin{cases} 1, & s_{\bmod(m,k)} \geqslant v_{\bmod(m,k)} > 0, \\ 0 & \text{в противном случае.} \end{cases}$$

Здесь используется обозначение $s_{\bmod m} = s - m\left[\frac{s}{m}\right]$ для наименьшего неотрицательного вычета s по модулю m.

Следствие 1.8. *Пусть случайное отображение* $f\colon S \to S$ *имеет распределение* (1) *на* Ω. *Тогда для любых фиксированных* $x, y \in S$, $x \neq y$, *и любого* $k \in \mathbb{N}$ *справедливо двустороннее неравенство*

$$\frac{1}{3k} < \lim_{n\to\infty} \mathbf{P}\left\{y \in \mathcal{K}_{f^k}(x)\right\} \leqslant \frac{2}{3}.$$

Теорема 1.12. *Пусть случайное отображение* $f\colon S \to S$ *имеет распределение* (1) *на* Ω. *Тогда для любых фиксированных* $x, y \in S$, $x \neq y$, *и любого* $k \in \mathbb{N}$ *справедливо равенство*

$$\mathbf{P}\left\{y \in \left(f^k\right)^{-1}(x)\right\} = \sum_{m \in \overline{Q}_2^n(k,1)} \frac{(n-2)_{m-2}}{n^m} + \sum_{t=1}^{n-1} \sum_{m=t+1}^{n} \frac{(n-2)_{m-2}}{n^m},$$

где $\overline{Q}_2^n(k,1) = \{2,\ldots,n\} \setminus Q_2^n(k,1)$ *определяется соотношением* (2).

Теорема 1.13. *Пусть случайное отображение $f\colon S \to S$ имеет распределение (1) на Ω. Тогда для любых фиксированных $x, y \in S$, $x \neq y$, и любого $k \in \mathbb{N}$ справедливо равенство*

$$\mathbf{P}\left\{f^k(x) = f^k(y)\right\} = \sum_{t=1}^{k}\sum_{s=0}^{n-1}\sum_{m=t+1}^{n-s}\frac{(1+\delta_{s,0})\,(n-2)_{m+s-2}}{n^{m+s}} + \\ + \sum_{t=1}^{k}\sum_{m=t+1}^{n}\sum_{i=0}^{t-1}\sum_{j=\delta_{i,0}}^{\left[\frac{k-t}{m-t}\right]}\frac{(n-2)_{m+i+jm-2}}{n^{m+i+jm}},$$

где $\delta_{i,j} = \begin{cases} 1, & i = j, \\ 0, & i \neq j, \end{cases}$ *— символ Кронекера.*

Приведенные результаты главы 1 диссертации могут быть использованы при синтезе и анализе современных итерационных АМЗИ типа «CryptoPro Key Meshing» (например, функций сжатия, хеш-функций, алгоритмов выработки производных ключей и генерации псевдослучайных последовательностей), а также обосновании выбора используемых в них параметров, существенно влияющих на теоретическую стойкость АМЗИ в целом.

Формулы для распределений исследованных в главе 1 случайных величин, заданных на множестве вершин графа G_{f^k}, в ряде случаев могут использоваться при построении критериев проверки статистических гипотез о видах распределений последовательностей, формируемых с использованием итерационных алгоритмов.

Во второй главе диссертации исследована структура графа композиции k независимых равновероятных случайных отображений конечного множества в себя, $k \in \mathbb{N}$. Для вероятностного пространства $(\Omega, \mathcal{F}, \mathbf{P})$ и независимых случайных отображений $f_1, \ldots, f_k$, имеющих распределение (1) на $\mathfrak{S}$, получены следующие результаты, описывающие теоретико-вероятностные свойства и характеристики графа $G_{f_{[k]}}$.

Через $F_{[k]}$ обозначим функцию распределения случайной величины $\tau_{f_{[k]}}(x)$ для произвольной фиксированной вершины $x \in S$.

Теорема 2.1. *Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \ldots, f_k$ независимы и имеют распределение (1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S$ и любого $z \in \{0, 1, \ldots, n\}$ справедливо равенство*

$$F_{[k]}(z) = 1 - \left(1 - \frac{z}{n}\right)\left(\frac{(n)_z}{n^z}\right)^k.$$

Следствие 2.2. *Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \ldots, f_k$ независимы и имеют распределение (1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S$, где*

$|S| = n$, *и любого* $u \geqslant 0$ *справедливо равенство*

$$\lim_{n\to\infty} \mathbf{P}\left\{\tau_{f_{[k]}}(x) > u\sqrt{2n}\right\} = e^{-ku^2}.$$

Следствие 2.3. *Пусть* $k \in \mathbb{N}$ *— произвольное, случайные отображения* $f_1, \ldots, f_k$ *независимы и имеют распределение* (1) *на* $\mathfrak{S}$. *Тогда для любого фиксированного* $x \in S$ *и любого* $z \in \{1, \ldots, n\}$ *справедливо равенство*

$$\mathbf{P}\left\{\tau_{f_{[k]}}(x) = z\right\} = \left(1 - \frac{z-1}{n} - \left(1 - \frac{z}{n}\right)\left(1 - \frac{z-1}{n}\right)^k\right)\left(\frac{(n)_{z-1}}{n^{z-1}}\right)^k.$$

Через $C\left(G_{f_{[k]}}\right)$ обозначим множество циклических вершин графа $G_{f_{[k]}}$, а через $C_l\left(G_{f_{[k]}}\right)$ — множество вершин графа $G_{f_{[k]}}$, лежащих на циклах длины $l \in \{1, \ldots, n\}$.

Теорема 2.2. *Пусть* $k \in \mathbb{N}$ *— произвольное, случайные отображения* $f_1, \ldots, f_k$ *независимы и имеют распределение* (1) *на* $\mathfrak{S}$. *Тогда для любого фиксированного* $x \in S$ *и любого* $l \in \{1, \ldots, n\}$ *справедливы равенства*

$$\mathbf{P}\left\{x \in C_l\left(G_{f_{[k]}}\right)\right\} = \frac{1}{n}\left(\frac{(n)_l}{n^l}\right)^k, \quad \mathbf{P}\left\{x \in C\left(G_{f_{[k]}}\right)\right\} = \frac{1}{n}\sum_{l=1}^{n}\left(\frac{(n)_l}{n^l}\right)^k.$$

Через $\lambda_{f_{[k]}}$ обозначим случайную величину, равную общему количеству циклических вершин в графе $G_{f_{[k]}}$.

Следствие 2.6. *Пусть* $k \in \mathbb{N}$ *— произвольное, случайные отображения* $f_1, \ldots, f_k$ *независимы и имеют распределение* (1) *на* $\mathfrak{S}$. *Тогда для любого* $l \in \{1, \ldots, n\}$

$$e^{-k\left(1+\frac{l}{n}\right)\frac{l(l-1)}{2n}} \leqslant \mathbf{E}\lambda_{f_{[k]}}(l) \leqslant e^{-k\frac{l(l-1)}{2n}}, \quad \mathbf{E}\lambda_{f_{[k]}} < 1 + \sqrt{\frac{\pi n}{2k}}.$$

Если при этом $n \to \infty$, *то* $\mathbf{E}\lambda_{f_{[k]}} = (1 + o(1))\sqrt{\frac{\pi n}{2k}}$.

Теорема 2.4. *Пусть* $k \in \mathbb{N}$ *— произвольное, случайные отображения* $f_1, \ldots, f_k$ *независимы и имеют распределение* (1) *на* $\mathfrak{S}$. *Тогда для любого фиксированного* $x \in S$ *и любых* $t \in \{1, \ldots, n-1\}$, $l \in \{1, \ldots, n-t\}$

$$\mathbf{P}\left\{x \in H^{(t,l)}_{f_{[k]}}\right\} = \left(\frac{1}{t+l-1} - \frac{1}{n}\right)\left(1 - \left(1 - \frac{t+l-1}{n}\right)^k\right)\left(\frac{(n)_{t+l-1}}{n^{t+l-1}}\right)^k.$$

Для произвольных $k \in \mathbb{N}$, $m, s_1, \ldots, s_k \in \mathbb{N}$, $n \geqslant m \geqslant s_1 \geqslant \ldots \geqslant s_k$, и произвольных

фиксированных различных $y_1, \ldots, y_m \in S$ определим событие

$$D^{\{k\}}_{s_1,\ldots,s_k}(y_1,\ldots,y_m) = \bigcap_{i=1}^{k} \left\{ \left| \left\{ f_{[i]}(y_1), \ldots, f_{[i]}(y_m) \right\} \right| = s_i \right\}.$$

Лемма 2.1. *Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \ldots, f_k$ независимы и имеют распределение (1) на $\mathfrak{S}$. Тогда для любых $m, s_1, \ldots, s_k \in \mathbb{N}$, $n \geqslant m \geqslant s_1 \geqslant \ldots \geqslant s_k$, и любых фиксированных различных $y_1, \ldots, y_m \in S$ справедливо равенство*

$$\mathbf{P}\left\{ D^{\{k\}}_{s_1,\ldots,s_k}(y_1,\ldots,y_m) \right\} = q(m, s_1) \prod_{i=1}^{k-1} q(s_i, s_{i+1}),$$

где $q(a,b) = C_n^{n-b} \left(\frac{b}{n}\right)^a \sum_{l=0}^{b} C_b^l (-1)^l \left(1 - \frac{l}{b}\right)^a$.

Теорема 2.5. *Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \ldots, f_k$ независимы и имеют распределение (1) на $\mathfrak{S}$. Тогда для любых фиксированных $x, y \in S$, $x \neq y$, справедливо равенство*

$$\mathbf{P}\left\{ f_{[k]}(x) = f_{[k]}(y) \right\} = \sum_{\substack{s_1,\ldots,s_{k-1}: \\ 2 \geqslant s_1 \geqslant \ldots \geqslant s_{k-1}}} \frac{q(2, s_1)}{n^{s_{k-1}-1}} \prod_{i=1}^{k-2} q(s_i, s_{i+1}).$$

Теорема 2.6. *Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \ldots, f_k$ независимы и имеют распределение (1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S$ справедливо равенство*

$$\mathbf{P}\left\{ x \in f_{[k]}(S) \right\} = \frac{1}{n} \sum_{l=1}^{n} \left(\frac{(n)_l}{n^l} \right)^k + \\ + \sum_{l=1}^{n-2} \sum_{t=1}^{n-l-1} \sum_{m=1}^{n-t-l} (-1)^{m-1} C_{n-1}^{m} \sum_{\substack{s_1,\ldots,s_{k-1}: \\ m \geqslant s_1 \geqslant \ldots \geqslant s_{k-1}}} \frac{q(m, s_1)}{n^{s_{k-1}}} \prod_{i=1}^{k-2} q(s_i, s_{i+1}) V^{\{k,m\}}_{s_1,\ldots,s_{k-1}},$$

где

$$V^{\{k,m\}}_{s_1,\ldots,s_{k-1}} = \frac{1}{n} \prod_{i=m+1}^{t+l+m-1} \left(1 - \frac{i}{n}\right) \cdot \prod_{i=1}^{k-1} \prod_{j=s_i+1}^{t+l+s_i-2} \left(1 - \frac{j}{n}\right) \cdot \sum_{v=0}^{k-1} \prod_{u=1}^{v} \left(1 - \frac{t+l+s_u-1}{n}\right).$$

Теорема 2.7. *Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \ldots, f_k$ независимы и имеют распределение (1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S \backslash S'$ и любых $r \in \{1, \ldots, n-1\}$, $S' \subseteq S$, $|S'| = r$, и $z \in \{1, \ldots, n\}$ справедливо равенство*

$$\mathbf{P}\left\{\tau_{f_{[k]}}(x)=z,\mathcal{R}_{f_{[k]}}(x)\cap S'=\varnothing\right\}=$$
$$=\left(1-\left(1-\frac{z}{n}\right)\left(1-\frac{z-1}{n}\right)^{k-1}\right)\left(\frac{(n)_{z-1}}{n^{z-1}}\right)^{k-1}\frac{(n)_{r+z}}{n^{z-1}(n)_{r+1}}.$$

Теорема 2.8. *Пусть $k\in\mathbb{N}$ — произвольное, случайные отображения $f_1,\ldots,f_k$ независимы и имеют распределение (1) на $\mathfrak{S}$. Тогда для любых фиксированных $x,y\in S$, $x\neq y$, справедливо равенство*

$$\mathbf{P}\left\{y\in\mathcal{K}_{f_{[k]}}(x)\right\}=1-\sum_{z=0}^{n-2}\left(1-\left(1-\frac{z+1}{n}\right)\left(1-\frac{z}{n}\right)^{k-1}\right)\left(\frac{(n)_z}{n^z}\right)^k\frac{C_{n-z}^2}{C_n^2}+$$
$$+\sum_{z=1}^{n-1}\sum_{u=0}^{n-z-1}\chi_k(z,u),$$

где

$$\chi_k(z,u)=\left(\frac{(n)_{z+u}}{n^{z+u}}\right)^k\left(\sum_{t=1}^{k}\frac{z^2}{n(n-1)}\left(1-\frac{z+u}{n}\right)^t+\right.$$
$$+\sum_{s=2}^{k}\sum_{t=1}^{s-1}\frac{z(z-1)}{n(n-1)}\left(1-\frac{z+u-1}{n}\right)^{s-k}\left(1-\frac{z+u}{n}\right)^t+$$
$$\left.+\sum_{t=1}^{k-1}\sum_{s=1}^{t}\frac{(z-1)^2}{n(n-1)}\left(1-\frac{z+u-1}{n}\right)^{t-k}\left(1-\frac{z+u}{n}\right)^s\right).$$

Теорема 2.9. *Пусть $k\in\mathbb{N}$ — произвольное, случайные отображения $f_1,\ldots,f_k$ независимы и имеют распределение (1) на $\mathfrak{S}$. Тогда для любых фиксированных $x,y\in S$, $x\neq y$, и любого $r\in\{1,\ldots,n\}$ справедливо равенство*

$$\mathbf{P}\left\{y\in\left(f_{[k]}\right)^{-r}(x)\right\}=\frac{1}{n}\left(1-\frac{1}{n-1}\sum_{z\in Q_r\setminus\{1\}}\left(\frac{(n)_z}{n^z}\right)^k\right),$$

где $Q_r=\{m\in\mathbb{N}\colon m|r\}$.

Результаты главы 2 диссертации описывают строение и вероятностные свойства графа $G_{f_{[k]}}$, $k\geqslant 1$, существенно используемые в рамках синтеза и анализа итерационных АМЗИ при выработке производных ключей, в принцип функционирования которых заложено применение различных преобразований или источника случайности в каждый отдельный такт их работы.

В Заключении изложены основные результаты диссертации, сформулированы выводы и обозначены перспективные направления дальнейших исследований.

ЗАКЛЮЧЕНИЕ

Исследования, проведенные в настоящей диссертации, направлены на развитие математического аппарата, позволяющего адекватно описывать современные итерационные АМЗИ, а также обосновывать выбор значений параметров соответствующих алгоритмов, гарантирующих защиту обрабатываемой с их использованием информации.

В диссертации исследованы структуры графов кратной итерации одного равновероятного случайного отображения конечного множества в себя и композиции нескольких независимых равновероятных случайных отображений конечного множества в себя, а также их вероятностные свойства и характеристики, которые могут быть использованы при моделировании и обосновании теоретической стойкости итерационных АМЗИ при выработке производных ключей.

Перспективными направлениями дальнейших исследований модификаций равновероятных случайных отображений в области информационной безопасности являются:

- исследование свойств и характеристик кратной итерации композиции нескольких равновероятных случайных отображений как объекта моделирования алгоритмов выработки производных ключей, использующих различные преобразования, определяемые некоторым источником случайности в каждый такт их работы, и реализующих последовательность производных ключей на основе тактов, отобранных с некоторым фиксированным периодом,

- построение и исследование математических моделей итерационных древовидных режимов работы хеш-функций, построенных на основе случайных отображений и обеспечивающих эффективную обработку больших объемов данных, а также допускающих реализацию в распределенных вычислительных системах и сетях,

- исследования, связанные с оценкой качества псевдослучайных последовательностей, формируемых с использованием итерационных АМЗИ, в том числе построение соответствующих статистических критериев.

Благодарности. Автор выражает искреннюю благодарность научному руководителю доктору физико-математических наук, старшему научному сотруднику Зубкову Андрею Михайловичу за постановку задач и внимание к работе. Автор благодарит

доктора физико-математических наук, ведущего научного сотрудника отдела дискретной математики Математического института им. В.А. Стеклова Российской академии наук Михайлова Владимира Гавриловича за проявленный интерес к работе и научное сотрудничество.

РАБОТЫ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи, опубликованные в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность» и входящих в списки Scopus или RSCI WoS.

1. Зубков А. М., Миронкин В. О., "Распределение длины отрезка апериодичности в графе k-кратной итерации случайного равновероятного отображения", *Математические вопросы криптографии*, **8**:4 (2017), 63-74 (RSCI WoS, ИФ РИНЦ 2020: 0,327) (А.М. Зубкову принадлежат постановка задачи и научное руководство, В.О. Миронкиным получены основные результаты статьи).

2. Миронкин В. О., Михайлов В. Г., "О множестве образов k-кратной итерации равновероятного случайного отображения", *Математические вопросы криптографии*, **9**:3 (2018), 99-108 (RSCI WoS, ИФ РИНЦ 2020: 0,327) (В.Г. Михайлову принадлежит постановка задачи, В.О. Миронкиным получены основные результаты статьи).

3. Миронкин В. О., "Об оценках распределения длины отрезка апериодичности в графе k-кратной итерации равновероятного случайного отображения", *Прикладная дискретная математика*, **42** (2018), 6-17 (Scopus, RSCI WoS, ИФ РИНЦ 2020: 0,38).

4. Миронкин В. О., "Слои в графе k-кратной итерации равновероятного случайного отображения", *Математические вопросы криптографии*, **10**:1 (2019), 73-82 (RSCI WoS, ИФ РИНЦ 2020: 0,327).

5. Миронкин В. О., "Распределение длины отрезка апериодичности в графе композиции независимых равновероятных случайных отображений", *Математические вопросы криптографии*, **10**:3 (2019), 89-99 (RSCI WoS, ИФ РИНЦ 2020: 0,327).

6. Миронкин В. О., "Коллизии и инцидентность вершин компонентам в графе k-кратной итерации равновероятного случайного отображения", *Дискретная математика*, **31**:4 (2019), 38-52 (RSCI WoS, ИФ РИНЦ 2019: 0,685).

7. Миронкин В. О., “Слои в графе композиции независимых равновероятных случайных отображений”, *Математические вопросы криптографии*, **11**:1 (2020), 101-114 (RSCI WoS, ИФ РИНЦ 2020: 0,327).

8. Миронкин В. О., “Об образах и прообразах в графе композиции независимых равновероятных случайных отображений”, *Прикладная дискретная математика*, **49** (2020), 5-17 (Scopus, RSCI WoS, ИФ РИНЦ 2020: 0,38).