DOI 10.37882/2223-2966.2025.03.05

ОЦЕНКА ЭФФЕКТИВНОСТИ РАБОТЫ АНТИВИРУСНОЙ ПРОГРАММЫ, ОБЕСПЕЧИВАЮЩЕЙ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ ОТ БЫСТРОРАЗМНОЖАЮЩИХСЯ ВРЕДОНОСНЫХ ПРОГРАММ

EVALUATION OF THE EFFECTIVENESS OF AN ANTIVIRUS PROGRAM THAT ENSURES INFORMATION SECURITY FROM RAPIDLY MULTIPLYING MALWARE

I. Atlasov
G. Plotnikov
V. Elin

Summary. The article discusses the features of countering malicious software capable of reproducing its copies for some time. Special attention is paid to the problem of detection and destruction by some antivirus program for some time under the following scenarios: The antivirus program copes with the rate of malware reproduction and destroys it on some generation of copies, or the antivirus program does not cope with this task and the process of malware reproduction gets out of control. The article discusses the methodology for evaluating the performance of an antivirus program based on the proposed conditions.

Keywords: malware, probability, mathematical expectation, generating function.

Атласов Игорь Викторович
профессор, Московский университет МВД России имени В.Я. Кикотя
Плотников Герман Геннадьевич
профессор, Московский университет МВД России имени В.Я. Кикотя
gr175@mail.ru
Елин Владимир Михайлович
доцент, Московский университет МВД России имени В.Я. Кикотя; Финансовый университет при Правительстве Российской Федерации

Аннотация. В статье рассматриваются особенности противодействия вредоносному программному обеспечению, способному к воспроизведению своих копий в течение некоторого времени. Особое внимание уделено проблеме выявления и уничтожения некоторой антивирусной программой так же в течение некоторого времени при следующих вариантах развития ситуации: антивирусная программа справляется с темпом размножения вредоносной и на каком-то поколении копий уничтожает её, либо антивирусная программа не справляется с этой задачей и процесс размножения вредоносной выходит из-под контроля. В статье рассматривается методика оценки работы антивирусной программы исходя из предложенных условий.

Ключевые слова: вредоносное программное обеспечение, вероятность, математическое ожидание, производящая функция.

В современном мире, когда информационные технологии пронизывают все сферы человеческой жизни, вопрос обеспечения кибербезопасности становится критически важным [1]. Одним из главных элементов этой защиты является эффективная антивирусная защита различных информационных систем.

Требованиями регулятора установлена взаимосвязь между обеспечением информационной безопасности и определением совокупности информационных угроз [2].Специальными нормативными документы ФСТЭК России определяют необходимость выявления и классификации угроз, что позволяет разработать индивидуальные способы и методы обнаружения, ликвидации и предупреждения для каждого компонента вредоносного программного обеспечения, исходя из того условия, что любая вредоносная программа имеет собственное предназначение и создана для достижения определенной цели как по проникновению, так и по нанесению вреда информационной системе.

При этом государственный стандарт в области информационной безопасности, устанавливающий классификацию и перечень факторов, воздействующих на безопасность защищаемой информации, в целях обоснования угроз безопасности информации и требований по защите информации на объекте информатизации [3,4], определяя в качестве угрозы совокупность условий и факторов, создающих потенциальную или реально существующую опасность, нарушения безопасности информации, требует обращать особое внимание на возможность несанкционированного доступа к информации путем применения вирусов или другого вредоносного программного кода.

В профессиональной среде в качестве одной из классификаций вредоносного программного обеспечения

предлагается классификация по критериям функциональности [5]: исполнители (обладают точно заданной конечной логикой своего исполнения); распространители (по специфике распространения; помощники (функцией которых становится поддержание другого вредоносного программного обеспечения). Распределение конкретного вредоносного программного обеспечения по указанным классам представлено в табл. 1.

Таблица 1.

Классификация вредоносного программного обеспечения

Исполнители	Распространители	Помощники
Шифровальщик	Троян	Вирус
Локер	Червь	Логическая бомба
Стиллер	Программа удалённого доступа	Руткит
Спамер	Установщик	Буткит
Ботнет		Инициализатор
Очиститель		

В настоящее время к категории наиболее быстроразмножающегося вредоносного программного обеспечения следует относить отдельные программы, осуществляющие самокопирование без активных действий со стороны пользователей. Так, например SQL-Slammer, заразивший более 75 000 устройств, отправляет свой вредоносный код в поисках не защищенных антивирусными программами устройств по сгенерированным вредоносной программой случайным IP-адресам. Более современным примером вредоносного программного обеспечения данной категории выступает комбинация «червь + руткит» специально разработанная для эксплуатации уязвимостей в системах Linux. При этом руткит осуществляет воздействие на файлы операционной системы, а червь обеспечивает быстрое распространение фрагментов вредоносного кода.

При этом вредоносное программное обеспечение, относящееся к данной категории, обладает рядом признаков:

— проникают на компьютер, пользуясь ошибками и уязвимостями программ, работающих на компьютере и принимающих данные из сети в рамках реализации сетевых атак;
— саморазмножаются, проникая с заражённого компьютера на найденные в сети ещё незаражённые компьютеры;
— оказывают вредоносный эффект на текущем компьютере;
— реализует неустойчивую работу компьютеров сети (включая как зараженные, так и ещё не зараженные).

Рассматривая задачу антивирусной защиты программно-аппаратных комплексов, предположим, что в некоторой информационной системе появилась вредоносная программа, которая через определенные моменты времени воспроизводит сама себя в нескольких экземплярах, или детектируется и уничтожается антивирусной программой. Предположим, что вероятность воспроизведения $k, \left(k = 0,1,2,\ldots\right)$ вирусов в ближайшем поколении равна $f_k > 0, \sum_{k=0}^{\infty} f_k = 1$. Очевидно, числа f_k зависят от антивирусной программы. Будем рассматривать только те случаи, когда антивирусная программа детектирует вредоносную программу. Далее, возможны варианты: антивирусная программа не дает ей размножиться, и на каком-то поколении уничтожает ее, либо не справляется с этой задачей.

Оценка вероятности размножения вредоносной программы

Вероятности f_k можно вычислить следующим образом. Возьмем информационную систему, которая нуждается в защите. Запускаем одновременно вредоносную программу и средство защиты от этой вредоносной программы. Далее, следим до первого размножения вредоносной программы и считаем количество копий, которых она успела воспроизвести. И этот эксперимент проделываем m раз. Затем каждому числу копий k ставим в соответствие дробь, в числителе которой стоит благоприятных случаев (когда исходная программа создала k копий), в знаменателе общее число случаев — m. В результате получим число f_k. Остается каким-то образом оценить эти значения.

Далее, каждый новый временной срез вредоносной программы будем называть поколением. Количество вредоносных программ в n поколении обозначим через ζ_n. Вредоносные программы можно пронумеровать. Обозначим символом $\xi_i^{(j,n)}, 1 \le i \le \zeta_n$ количество вредоносных программ, произведенных от i вредоносной программы в n поколении в j эксперименте. Если проводится только один эксперимент, то вместо обозначения $\xi_i^{(1,n)}$ будем использовать обозначение $\xi_i^{(n)}$. Согласно условиям задачи, независимо от поколения k и номера i, вероятность того, что случайная величина $\xi_i^{(n)}$ примет значение n.

$$P\left(\xi_i^{(k)} = n\right) = f_n \qquad (1)$$

для всех натуральных n и нуля. По построению, мы считаем

$$f_k^{(m)} = \frac{1}{m}\sum_{j=1}^{m}\varphi_k\left(\xi_1^{(j,1)}\right)$$

где

$$\varphi_k(x) = \begin{pmatrix} 1, & x = k \\ 0, & x \neq k \end{pmatrix}$$

Если существует натуральное число k_0, такой что для некоторого $m > 10$ величины и всех $k > k_0$ выполнено равенство

$$f_k^{(m)} = f_k^{(2m)} = f_k^{(3m)} = 0$$

и, неравенство

$$f_{k-1}^{(m)} > 0$$

то с достаточно большой вероятностью можно утверждать, что ряды $\sum_{k=1}^{\infty} k f_k$ и $\sum_{k=1}^{\infty} k^2 f_k$ сходятся, то есть для случайной величины $\xi_i^{(k)}$ существует математическое ожидание и дисперсия.

Если такого k_0 не существует, то имеет смысл выбрать более надежную антивирусную программу.

Математическое обоснование методики подавления размножения вредоносных программ

Общая схема размножения преступлений выглядит следующим образом

$$\zeta_0 = 1, \zeta_1 = \xi_i^{(1)}, \zeta_2 = $$
$$= \begin{pmatrix} \sum_{i=1}^{\zeta_1} \xi_i^{(2)}, & \zeta_1 \geq 1 \\ 0, & \zeta_1 = 0 \end{pmatrix}, \ldots, \zeta_n = \begin{pmatrix} \sum_{i=1}^{\zeta_{n-1}} \xi_i^{(n)}, & \zeta_{n-1} \geq 1 \\ 0 & \zeta_{n-1} = 0 \end{pmatrix}$$

Заметим, что набор случайных величин $\left\{\xi_i^{(n)}\right\}_{i=1}^{\zeta_{n-1}}$ и ζ_{n-1} независим в совокупности.

Рассмотрим ряд гипотез

$$H_k = \{\zeta_n = k\}, k = 0,1,\ldots.$$

Очевидно, события $\{H_k\}_{k=0}^{\infty}$ образуют полную группу событий. Поэтому, для комплексного $z \in C$, $|z| \leq 1$ (C–множество комплексных чисел) и производящей функции $M\left(z^{\zeta_n}\right)$ [6] по формуле полной вероятности для математических ожиданий выполнены равенства

$$M\left(z^{\zeta_n}\right) = \sum_{k=0}^{\infty} M\left(z^{\zeta_n} / H_k\right) P(H_k) =$$
$$= P(\zeta_n = 0) + \sum_{k=1}^{\infty} z^k P(\zeta_n = k)$$

Обозначим

$$f_{(n)}(z) = M\left(z^{\zeta_n}\right)$$

Поэтому, справедливо равенство

$$f_{(n)}(0) = M\left(z^{\zeta_n}\right)\Big|_{z=0} =$$
$$= P(\zeta_n = 0) + \sum_{k=1}^{\infty} P(\zeta_n = k) 0^k = \quad (2)$$
$$= P(\zeta_n = 0)$$

Рассмотрим ряд гипотез

$$G_k = \{\zeta_{n-1} = k\}, k = 0,1,\ldots.$$

Очевидно, события $\{G_k\}_{k=0}^{\infty}$ образуют полную группу событий. По формуле полной вероятности [7] имеем

$$M\left(z^{\zeta_n}\right) = \sum_{k=0}^{\infty} M\left(z^{\zeta_n} / G_k\right) P(G_k) =$$
$$\sum_{k=0}^{\infty} M\left(z^{\sum_{i=1}^{\zeta_{n-1}} \xi_i^{(n)}} / \zeta_{n-1} = k\right) P(\zeta_{n-1} = k) =$$
$$\sum_{k=0}^{\infty} M\left(z^{\sum_{i=1}^{k} \xi_i^{(n)}} / \zeta_{n-1} = k\right) P(\zeta_{n-1} = k) =$$
$$\sum_{k=0}^{\infty} M\left(\prod_{j=0}^{k} z^{\xi_j^{(n)}}\right) P(\zeta_{n-1} = k)$$

Из независимости набора случайных величин $\left\{\xi_i^{(n)}\right\}_{i=1}^{\zeta_{n-1}}$ и ζ_{n-1} в совокупности и определения математического ожидания следует, что

$$M\left(z^{\zeta_n}\right) = \sum_{k=0}^{\infty} \prod_{j=0}^{k} M\left(z^{\xi_j^{(n)}}\right) P(\zeta_{n-1} = k) =$$
$$\sum_{k=0}^{\infty} \left(M\left(z^{\xi_1^{(n)}}\right)\right)^k P(\zeta_{n-1} = k) =$$
$$M\left(\left(M\left(z^{\xi_1^{(n)}}\right)\right)^{\zeta_{n-1}}\right).$$

Итак, доказана формула

$$f_{(n)}(z) = M\left(z^{\zeta_n}\right) = M\left(\left(M\left(z^{\xi_1^{(n)}}\right)\right)^{\zeta_{n-1}}\right) \quad (3)$$

Согласно формуле (1), для любого k можно корректно использовать обозначения для производящей функции [7]

$$f(z)=f_{(1)}(z) = M\left(z^{\xi_1^{(1)}} \right) = M\left(z^{\xi_1^{(k)}} \right) = \sum_{k=0}^{\infty} f_k z^k \quad (4)$$

Тогда формула (3) примет вид

$$f_{(n)}(z) = M\left(z^{\zeta_n}\right) = M\left(\left(M\left(z^{\xi_1^{(n)}} \right) \right)^{\zeta_{n-1}} \right) = f_{(n-1)}\left(f(z)\right)$$

Подставляя и далее в эту формулу, получим,

$$f_{(n)}(z) = f_{(n-1)}\left(f(z)\right) = f_{(n-2)}\left(f\left(f(z)\right)\right) =$$

$$f_{(n-3)}\left(f\left(f\left(f(z)\right)\right)\right) = \ldots = \underbrace{f\ldots\left(f\left(f(z)\right)\right)}_{n}$$

Обозначим

$$f_2(z) = f\left(f(z)\right),$$

$$f_3(z) = f\left(f_2(z)\right) = f\left(f\left(f(z)\right)\right), \ldots$$

$$f_k(z) = f\left(f_{k-1}(z)\right) = \underbrace{f\ldots\left(f\left(f(z)\right)\right)}_{k}$$

Используя эти обозначения, получим равенства

$$f_{(n)}(z) = f_n(z) = f\left(f_{n-1}(z)\right) \quad (5)$$

Обоснование существования процесса вырождения вредоносных программ

Найдем вероятность вырождения процесса, то есть вероятность того, что антивирусная программа не даст размножаться вредоносной программе и уничтожит ее. Это означает наступление событие, состоящее в том, что начиная с некоторого номера n все $\zeta_n = 0$. Если $\zeta_n = 0$, то для всех $k = 1,2,\ldots \zeta_{n+k} = 0$, или преступления больше не размножаются. Это следует из того, что

$$P\left(\zeta_{n+1} = 0 \,/\, \zeta_n = 0\right) = 1.$$

Обозначим $A_k = \left\{\zeta_k = 0\right\}$. В этом случае вырождение представляет собой событие $k = 1 \infty A_k$. Так как $A_n \subset A_{n+1}$, то из теоремы Вейерштрассе (монотонное возрастание последовательности $P\left(A_n\right)$ и ограниченность $P\left(A_n\right) \le 1$) следует существование предела (вероятность вырождения) $q \le 1$

$$q = P\left(k = 1 \middle| \infty A_k\right) = \lim_{n\to\infty} P\left(A_n\right).$$

Рассмотрим случайную величину $\xi_i^{(k)}$.

Теорема 1. *Пусть у случайной величины $\xi_i^{(k)}$ конечны моменты первого и второго порядка, тогда вероятность вырождения q равна наименьшему неотрицательному корню уравнения $q = f(q)$.*

Proof. Прежде всего заметим, что число 1 всегда является корнем уравнения $q = f(q)$. Имеем,

$$f(1) = \sum_{k=0}^{\infty} f_k = 1$$

Из формул (2), (5) имеем

$$P\left(A_n\right) = f_n(0) = f_{(n)}(0) \le 1$$

Из вложения $A_n \subset A_{n+1}$ следует, что

$$f_n(0) = P\left(A_n\right) \le P\left(A_{n+1}\right) = f_{n+1}(0) \le 1 \quad (6)$$

Как замечено выше, согласно теореме Вейерштассе, существует конечный предел

$$\lim_{n\to\infty} f_n(0) = q \le 1. \quad (7)$$

Заметим, что для $|z| < 1$ ряд $\sum_{k=0}^{\infty} f_k |z|^k$ мажорируется сходящимся рядом $\sum_{k=0}^{\infty} f_k$. Отсюда следует его равномерная сходимость. Следовательно, для $|z| < 1$ ряд $\sum_{k=0}^{\infty} f_k z^k$ является непрерывной функцией. Перейдя в равенстве

$$f_n(0) = f\left(f_{n-1}(0)\right) \quad (8)$$

к пределу при $n \to \infty$ получим равенство

$$q = f(q). \quad (9)$$

Так как у случайной величины $\xi_i^{(k)}$ конечен момент первого порядка, то для $|z| < 1$ ряд $\sum_{k=0}^{\infty} k f_k |z|^{k-1}$ мажорируется сходящимся рядом $\sum_{k=0}^{\infty} k f_k$. Отсюда следует его равномерная сходимость и возможность почленного дифференцирования

$$f\ (x) = \sum_{k=1}^{\infty} k f_k x^{k-1} > 0$$

Доказано, что функция $f(x)$ не убывает.

Так как у случайной величины $\xi_i^{(k)}$ конечен момент второго порядка, то для $|z| < 1$ ряд $\sum_{k=0}^{\infty} k(k-1) f_k |z|^{k-2}$ мажорируется сходящимся рядом

$$\sum_{k=0}^{\infty} k(k-1) f_k \le \sum_{k=0}^{\infty} k^2 f_k < \infty.$$

Отсюда следует его равномерная сходимость и возможность почленного дифференцирования

$$f^{*}(x)=\sum_{k=2}^{\infty}k(k-1)f_k x^{k-2}>0$$

Доказано, что функция $f(x)$ выпукла.

Заметим, что число

$$m = f\ (1) = \sum_{k=1}^{\infty} k f_k = M\left(\xi_1^{(1)}\right)$$

является средним значение случайной величины $\xi_1^{(1)}$, то есть средняя величина потомства.

Рассмотрим несколько случаев.

1. Пусть $f_1 = P\left(\xi_1^{(1)} = 1\right) < 1$. И для этого случая рассмотрим несколько случаев.

(a) Пусть $m = f\ (1) \le 1$, тогда для $0 < x < 1$ для неубывающей и выпуклой функции $f(x)$ имеем $f(x) > x$. То есть $q = 1$ и процесс вырождается с вероятностью 1.

(b) Пусть $m = f\ (1) > 1$, тогда для x близких к 1 справедливо неравенство

$$f(x) < x \tag{10}$$

Очевидно, на отрезке $0 < x < 1$ неубывающая и выпуклая функции $f(x)$ имеет либо два корня $q \le 1$ и 1, либо один корень равный 1.

Покажем, что последовательность $f_n(0)$ не может стремиться к 1. То есть случай (a) точно не выполняется. Предположим противное. Пусть уравнение (9) имеет корень $q = 1$. Из равенства (6) и предположения следует, что последовательность $f_n(0)$ монотонно возрастая стремится к единице. Тогда последовательность $\delta_n = 1 - f_n(0)$ монотонно убывая стремится к нулю. Из непрерывности функции $f(x)$ и неравенства (10) следует, что для достаточно больших n справедливо неравенство

$$f(1-\delta_n) < 1 - \delta_n. \tag{11}$$

Из неравенства (8) имеем

$$f_{n+1}(0) = f\left(f_n(0)\right) = f\left(1-\left(1-f_n(0)\right)\right) = f(1-\delta_n)$$

Поэтому, из неравенства (11), для достаточно больших n, имеем

$$\delta_{n+1} = 1 - f_{n+1}(0) = 1 - f(1-\delta_n) > \delta_n.$$

Что противоречит монотонности убывания последовательности δ_n. Итак, доказано, что случай (a) не выполняется и корень уравнения (9) равен $q < 1$.

2. Рассмотрим случай, когда $f_1 = P\left(\xi_1^{(1)} = 1\right) = 1$. В этом случае

$$f(x) = f_1 x \equiv x.$$

Так как $f_0 = P\left(\xi_0^{(n)} = 0\right) = 0$, то процесс не может выродиться и, следовательно, $q = 0$. Заметим, что q является наименьшим корнем уравнения $f(x) = x$.

Описание методики по оценке работы антивирусной программы

Итак, общая модель оценки работы антивирусной программы имеет вид

1. Вычисляем значение

$$m = \sum_{k=0}^{\infty} k f_k \tag{12}$$

Если $m < 1$, то процесс вырождается с единичной вероятностью.

Вывод: при $m < 1$ антивирусной программы можно считать идеальной, в виду того, что число новых копий вредоносной программы будет безальтернативно сокращаться с вероятностью равной единице.

2. Пусть $m > 1$. Задаем некоторое α близкое к единице и ε близкое к нулю.

Далее, как сказано выше, существует число $0 < q < 1$, являющееся вероятностью вырождения, такое что для функции

$$f(z) = \sum_{k=0}^{\infty} f_k z^k, z \in C \tag{13}$$

справедливо равенство (9)

$$q = f(q) = \sum_{k=0}^{\infty} f_k q^k.$$

Согласно (7) для нахождения q можно воспользоваться рекуррентным соотношением (8)

$$q_0 = 0, q_1 = f(q_0), q_n = f(q_{n-1}) \tag{14}$$

Как сказано выше, последовательность q_n монотонно возрастает и стремится к q. Приближенное вычисление $q \approx q_n$ останавливается при выполнении условия [?]

$$\left|q_{n+1} - q_n\right| = \left|f\left(q_n\right) - q_n\right| < \varepsilon \qquad (15)$$

для некоторого достаточно малого $\varepsilon > 0$.

Вывод: если $m > 1$ и $q > \alpha$, то работу антивирусной программы можно считать удовлетворительной, в виду того, что число новых копий вредоносной программы будет только сокращаться с вероятностью близкой к единице — $q \approx 1$.

Таким образом, следует обращать особое внимание на возможность несанкционированного доступа к информации путем применения вирусов или другого вредоносного программного кода, к категории наиболее быстроразмножающегося вредоносного программного обеспечения следует относить отдельные программы, осуществляющие самокопирование без активных действий со стороны пользователей Антивирусная защита различных информационных систем является одним из главных элементов защиты критической информационной инфраструктуры. При этом актуальными сценариями противодействия компьютерным атакам выступают следующие варианты развития ситуации: антивирусная программа справляется с темпом размножения вредоносной и на каком-то поколении копий уничтожает её, либо антивирусная программа не справляется с этой задачей и процесс размножения вредоносной выходит из-под контроля. Произведенными расчетами произведена оценка вероятности размножения вредоносной программы; а также математическое обоснование методики подавления размножения вредоносных программ.

На основании проведенных расчетов обосновано существование процесса вырождения вредоносных программ, т. е. вероятность того, что антивирусная программа не даст размножаться вредоносной программе и уничтожит ее. Математически доказано, что работу антивирусной программы можно считать удовлетворительной, в виду того, что число новых копий вредоносной программы будет только сокращаться с вероятностью близкой к единице.

ЛИТЕРАТУРА

1. Жарова А.К. Обеспечение суверенитета Российской Федерации в информационной сфере / А.К. Жарова // Государственная власть и местное самоуправление. — 2024. — № 9. — С. 41–45. — DOI 10.18572/1813–1247-2024-9-41-45. — EDN MTSBWP.
2. Об утверждении требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Приказ ФСТЭК России от 11 февр. 2013 г. № 17 // Официальный сайт ФСТЭК России. 61 URL: http://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya2013-g-n-17 (дата обращения: 22.06.2016).
3. ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. М.: Стандартинформ, 2007. 7 с.
4. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. М.: Стандартинформ, 2007. 12 с.
5. Классификация вредоносного ПО на основе композиций и комбинирования//https://habr.com/ru/articles/748254/
6. Гнеденко Б.В. Курс теории вероятностей. М.: УРСС, 2001.
7. Боровков А.А. Теория вероятностей. М.: Наука, 1986.
8. Крамер Г. Математические методы статистики Москва, Мир, 1976.
9. Андерсон Т.В.Г. Введение в многомерный статистический анализ Москва, Физматгиз, 1963.
10. Бартлетт М.С.Г. On the theory of statistical regression Proc. Roy. Soc. Edinburgh. — 1933.— V. 53.— P. 260–283
11. Гантмахер Ф.Р. Теория матриц. М.: Наука, 1966.
12. Гнеденко Б.В., Колмогоров А.Н. Предельные распределения для сумм независимых случайных величин. М.: Гостехиздат, 1949.
13. Головина Л.И. Линейная алгебра и некоторые ее приложения. М.: Наука, 1975.
14. Колмогоров А.Н. Grundbegriffe der Wahrscheinlichkeitsrechnung. Springer-Verlag, 1933. [Рус. пер.: Основные понятия теории вероятностей. — М.: ОНТИ, 1936; М.: Наука, 1974.]
15. Колмогоров А.Н., Фомин СВ. Элементы теории функций и функционального анализа. М.: Наука, 1972.