DOI 10.37882/2223-2966.2024.6-2.07

ОЦЕНКА ЭФФЕКТИВНОСТИ РАБОТЫ АНТИВИРУСНЫХ ПРОГРАММ ПО ЗАЩИТЕ ИНФОРМАЦИИ

EVALUATION OF THE EFFECTIVENESS OF ANTI-VIRUS PROGRAMS TO PROTECT INFORMATION

I. Atlasov
G. Plotnikov
V. Elin
E. Zaripova

Summary. Currently, federal executive authorities have defined [1] a list of requirements for anti-virus protection tools, as well as protection profiles for anti-virus protection tools of protection classes 1, 2 and 3, which necessitates the development of a methodology for determining the effectiveness of various anti-virus programs based on the results of processing the proposed set of parameters.

The basis of this study is the possibility of installing such an antivirus program on an information system, which allows you to identify incidents related to the use of malicious software, track and destroy malicious software for some time. At the same time, the limitation of the functionality of the presented antivirus program determines the inability to respond to new impacts within the stated time.

The task of this work is to find the probability of occurrence of an event for an arbitrary time interval, which consists in the ability to count and destroy all harmful effects.

Keywords: information security, threat detection models, counteraction to threats, statistical methods of information security.

Атласов Игорь Викторович
Д.н., профессор,
Московский университет МВД России имени В.Я. Кикотя
Плотников Герман Геннадьевич
Д.н., профессор,
Московский университет МВД России имени В.Я. Кикотя
gr175@mail.ru
Елин Владимир Михайлович
К.п.н., доцент,
Московский университет МВД России имени В.Я. Кикотя;
Финансовый университет при Правительстве Российской Федерации, Москва
elin_VM@mail.ru
Зарипова Эльвира Ринатовна
К.н., доцент,
Московский университет МВД России имени В.Я. Кикотя;
МИРЭА — Российский технологический университет
ezarip@gmail.com

Аннотация. В настоящее время федеральными органами исполнительной власти определен [1] перечень требований к средствам антивирусной защиты, а также профили защиты средств антивирусной защиты 1, 2 и 3 классов защиты, в связи с чем возникает необходимость разработки методики определения эффективности различных антивирусных программ по результатам обработки предлагаемой совокупности параметров.

В основу настоящего исследования положена возможность установки на информационную систему такой антивирусной программы, которая позволяет выявить инциденты, связанные с применением вредоносного программного обеспечения, отследить и уничтожить вредоносное программное обеспечение в течение некоторого времени τ. При этом ограничением функциональности представленной антивирусной программы определена невозможность реагировать на новые воздействия в течение заявленного времени τ.

Задачей настоящей работы выступает нахождение вероятности наступления события для произвольного времени t на интервале $[0, t]$, заключающегося в возможность сосчитать и уничтожить все вредоносные воздействия.

Ключевые слова: информационная безопасность, модели выявления угроз, противодействие угрозам, статистические методы информационной безопасности.

Постановка задачи и ограничения на нее

По результатам ряда экспериментов получено статистически достоверное число атак вредоносных компьютерных программ на информационную систему на единичном интервале времени, используемое в качестве делимого. В качестве делителя задано число неудачных экспериментов, при которых в течение заданного отрезка времени наступил инцидент, выражающийся хотя бы в единичном вредоносном воздействии [2;3].

Представлено также среднее время обработки вредоносного воздействия (взятое из характеристик антивирусной программы). Выбирая некоторое (в зависимости от эффективности работы антивирусной программы необходимой нам для оценивания больших или малых

промежутков времени), число из статистических выводов следует определить антивирусную программу с наиболее высокими показателями.

Найдем вероятность обнаружения вредоносных воздействий на промежутке времени $[0,t]$. Обозначим через $A(t_1,t_2)$, событие, состоящее в том, что на интервале времени $[t_1,t_2]$ все вредоносные воздействия сосчитаны. Через $B_k^{(t_1,t_2)}$ событие, состоящее в том, что прошло ровно k вредоносных воздействий за интервал времени $[t_1,t_2]$. Через $B_{>1}^{(t_1,t_2)}$ событие, состоящее в том, что прошло более 1 вредоносного воздействия за интервал времени $[t_1,t_2]$. Обозначим $\pi(t) = P(A(0,t))$.

Обозначим символом p_0 вероятность того, что на интервале $[0,1]$ не произошло ни одного события

$$p_0 = P\left(B_0^{(0,1)}\right), a = -ln\left(P\left(B_0^{(0,1)}\right)\right).$$

Появление вредоносного воздействия будем в дальнейшем называть событием. Относительно появления вредоносных воздействий предположим следующее:

1. Вероятность появления более одного события за бесконечно малый промежуток времени является бесконечно малой величиной

$$P\left(B_{>1}(t_1,t_1+\Delta t)\right) = o(\Delta t).$$

2. Функция $\pi(t)$ непрерывна на интервале $[0,\infty]$ и $\pi(0) = 1$.
3. Вероятность появления не одного события за бесконечно малый промежуток времени является бесконечно близкой к единице величиной

$$P\left(B_0^{(t_1,t_1+\Delta t)}\right) = 1 + o(\Delta t).$$

4. Вероятности появления одинакового числа событий за равные по длине промежутки времени совпадают

$$P\left(B_k^{(t_1,t_1+\Delta t)}\right) = P\left(B_k^{(t_2,t_2+\Delta t)}\right).$$

5. События, произошедшие за непересекающиеся промежутки времени, независимы. Пусть $t_2 \le t_3$. В этом случае

$$P\left(B_k^{(t_1,t_2)} \cap B_m^{(t_3,t_4)}\right) = P\left(B_k^{(t_1,t_2)}\right)P\left(B_m^{(t_3,t_4)}\right).$$

Для натурального m из свойства 3 и 2, имеем

$$P\left(B_0^{(0,m)}\right) = P\left(\prod_{k=0}^{m-1} B_0^{(k,k+1)}\right) =$$
$$= \prod_{k=0}^{m-1} P\left(B_0^{(k,k+1)}\right) = \prod_{k=0}^{m-1} P\left(B_0^{(0,1)}\right) = p_0^m.$$

Разделим интервал $[0,m]$ на n равных частей. Из свойств 2 и 3 имеем

$$P\left(B_0^{(0,m)}\right) = P\left(\prod_{k=0}^{n-1} B_0^{\left(\frac{km}{n},\frac{(k+1)m}{n}\right)}\right) =$$
$$= \prod_{k=0}^{n-1} P\left(B_0^{\left(\frac{km}{n},\frac{(k+1)m}{n}\right)}\right) = \prod_{k=0}^{n-1} P\left(B_0^{\left(0,\frac{m}{n}\right)}\right) =$$
$$= P^n\left(B_0^{\left(0,\frac{m}{n}\right)}\right) = p_0^m.$$

Отсюда следует, что

$$P\left(B_0^{\left(0,\frac{m}{n}\right)}\right) = p_0^{\frac{m}{n}}.$$

Для любого $s \in R$ можно подобрать монотонную возрастающую последовательность рациональных чисел $s_k = \frac{m_k}{n_k}$, такую что

$$|s - s_k| \underset{k\to\infty}{\to} 0.$$

В этом случае,

$$P\left(B_0^{(0,s)}\right) = P\left(B_0^{(0,s_k)} \cap B_0^{(s_k,s)}\right) =$$
$$= P\left(B_0^{\left(0,\frac{m}{n}\right)}\right)P\left(B_0^{(s_k,s)}\right) = p_0^{s_k}P\left(B_0^{(0,s-s_k)}\right).$$

По условию задачи при $|s - s_k| \underset{k\to\infty}{\to} 0$ справедливо условие

$$P\left(B_0^{(0,s-s_k)}\right) \underset{k\to\infty}{\to} 1.$$

Поэтому, из ряда Тейлора следует

$$P\left(B_0^{(0,s)}\right) = \lim_{k\to\infty}\left(p_0^{s_k}P\left(B_0^{(s-s_k)}\right)\right) =$$
$$= \lim_{k\to\infty} p_0^{s_k} \lim_{k\to\infty} P\left(B_0^{(s-s_k)}\right) \underset{k\to\infty}{\to} p_0^s = \quad (1)$$
$$= e^{-s(-\ln p_0)} \overset{def}{=} e^{-as} = 1 - as + o(s).$$

Заметим, что

$$P\left(B_0^{(t_1,t_2)} \cup B_1^{(t_1,t_2)} \cup B_{>1}^{(t_1,t_2)}\right) =$$
$$= P\left(B_0^{(t_1,t_2)}\right) + P\left(B_1^{(t_1,t_2)}\right) + P\left(B_{>1}^{(t_1,t_2)}\right) = 1.$$

Так как

$$P\left(B_{>1}^{(t_1,t_2)}\right) = P\left(B_{>1}^{(0,t_2-t_1)}\right) = o(t_2 - t_1),$$

то

$$P\left(B_1^{(t_1,t_2)}\right) = P\left(B_1^{(0,t_2-t_1)}\right) = a\left(t_2 - t_1\right) + o\left(t_2 - t_1\right).$$

Окончательно, имеем

$$\begin{aligned} &P\left(B_0^{(t_1,t_2)}\right) = P\left(B_0^{(0,t_2-t_1)}\right) \overset{def}{=} e^{-a(t_2-t_1)} = \\ &= 1 - a\left(t_2 - t_1\right) + o\left(t_2 - t_1\right) \\ &P\left(B_1^{(t_1,t_2)}\right) = P\left(B_1^{(0,t_2-t_1)}\right) = a\left(t_2 - t_1\right) + o\left(t_2 - t_1\right) \\ &P\left(B_{>1}^{(t_1,t_2)}\right) = P\left(B_{>1}^{(0,t_2-t_1)}\right) = o\left(t_2 - t_1\right) \end{aligned} \quad (2)$$

Решение задачи

Рассмотрим ряд случаев.

Пусть $0 < t < \tau$ и $\Delta t > 0$. Рассмотрим рисунок ниже

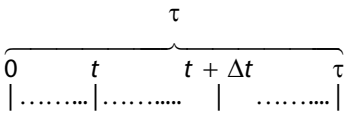

Рис. 1

Имеем

$$\begin{aligned} &A\left(0,t+\Delta t\right) = \\ &= B_0^{(0,t)}B_1^{(t,t+\Delta t)} + B_0^{(0,t)}B_0^{(t,t+\Delta t)} + B_1^{(0,t)}B_0^{(t,t+\Delta t)} = \\ &= B_0^{(0,t)}B_1^{(t,t+\Delta t)} + B_0^{(t,t+\Delta t)}\left[B_0^{(0,t)} + B_1^{(0,t)}\right]. \end{aligned} \quad (3)$$

Очевидно, что

$$A\left(0,t\right) = B_0^{(0,t)} + B_1^{(0,t)}.$$

Поэтому, равенство (3) превращается в равенство

$$A\left(0,t+\Delta t\right) = B_0^{(0,t)}B_1^{(t,t+\Delta t)} + B_0^{(t,t+\Delta t)}A\left(0,t\right). \quad (4)$$

Заметим, что события $A\left(0,t\right)B_0^{(t,t+\Delta t)}$ и $B_0^{(0,t)}B_1^{(t,t+\Delta t)}$ несовместимы, так как противоположены события $B_0^{(t,t+\Delta t)}$ и $B_1^{(t,t+\Delta t)}$. Поэтому,

$$\begin{aligned} &P\left(A\left(0,t+\Delta t\right)\right) = \\ &= P\left(B_0^{(0,t)}B_1^{(t,t+\Delta t)}\right) + P\left(B_0^{(t,t+\Delta t)}A\left(0,t\right)\right). \end{aligned} \quad (5)$$

По условию задачи, события $A\left(0,t\right)$ и $B_0^{(t,t+\Delta t)}$ независимы. Также независимы события $B_0^{(0,t)}$ и $B_1^{(t,t+\Delta t)}$. Поэтому, из (5) следует что

$$\begin{aligned} &P\left(A\left(0,t+\Delta t\right)\right) = \\ &= P\left(B_0^{(0,t)}\right)P\left(B_1^{(t,t+\Delta t)}\right) + P\left(B_0^{(t,t+\Delta t)}\right)P\left(A\left(0,t\right)\right) = \\ &= P\left(B_0^{(0,t)}\right)P\left(B_1^{(t,t+\Delta t)}\right) + P\left(B_0^{(0,\Delta t)}\right)P\left(A\left(0,t\right)\right). \end{aligned} \quad (6)$$

Поэтому, из формул (3) и (6), получим

$$\pi\left(t+\Delta t\right) = \pi\left(t\right)\left(1 - a\Delta t\right) + e^{-at}a\Delta t$$

$$\frac{\pi\left(t+\Delta t\right) - \pi\left(t\right)}{\Delta t} = -a\pi\left(t\right) + ae^{-at}.$$

Устремляя Δt к нулю справа получим линейное неоднородное дифференциальное уравнение

$$\left.\frac{\partial\pi}{\partial t}\right|_{+0} = -a\pi\left(t\right) + ae^{-at}, \quad (7)$$

где символом $\left.\frac{\partial\pi}{\partial t}\right|_{+0}$ обозначена правосторонняя производная.

2. Пусть $0 < t < \tau$ и $\Delta t > 0$. В этом разделе также рассмотрим рисунок

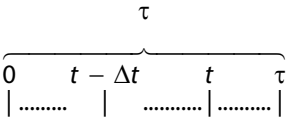

Рис. 2

Имеем

$$\begin{aligned} &A\left(0,t\right) = \\ &B_0^{(0,t-\Delta t)}B_1^{(t-\Delta t,t)} + B_0^{(0,t-\Delta t)}B_0^{(t-\Delta t,t)} + B_1^{(0,t-\Delta t)}B_0^{(t-\Delta t,t)} = \\ &= B_0^{(0,t-\Delta t)}B_1^{(t-\Delta t,t)} + B_0^{(t-\Delta t,t)}\left[B_0^{(0,t-\Delta t)} + B_1^{(0,t-\Delta t)}\right]. \end{aligned} \quad (8)$$

Очевидно, что

$$A\left(0,t-\Delta t\right) = B_0^{(0,t-\Delta t)} + B_1^{(0,t-\Delta t)}.$$

Поэтому, равенство (8) превращается в равенство

$$A\left(0,t\right) = B_0^{(0,t-\Delta t)}B_1^{(t-\Delta t,t)} + B_0^{(t-\Delta t,t)}A\left(0,t-\Delta t\right). \quad (9)$$

Из формулы (9), получим

$$\pi\left(t\right) = \pi\left(t-\Delta t\right)\left(1 - a\Delta t\right) + e^{-at}a\Delta t$$

$$\frac{\pi\left(t-\Delta t\right) - \pi\left(t\right)}{-\Delta t} = -a\pi\left(t-\Delta t\right) + ae^{-at}.$$

Устремляя Δt к нулю получим линейное неоднородное дифференциальное уравнение

$$\left.\frac{\partial\pi}{\partial t}\right|_{-0} = -a\pi\left(t\right) + ae^{-at}, \quad (10)$$

где символом $\left.\frac{\partial\pi}{\partial t}\right|_{-0}$ обозначена левосторонняя производная. Объединяя уравнения (7) и (10) получим дифференциальное уравнение

$$\frac{\partial\pi}{\partial t} = -a\pi\left(t\right) + ae^{-at}. \quad (11)$$

Так как начальное условие — $\pi(0) = 1$, состоящее в том, что все вредоносные воздействия в начальный момент времени подсчитаны с вероятностью 1, то получим решение

$$\pi(t) = e^{-at}(1 + at), t \in [0, \tau]. \qquad (12)$$

3. Пусть $\tau < t < 2\tau$ и $\Delta t > 0$, $n \in N$. В дальнейшем, в этом разделе, будем пользоваться рисунком

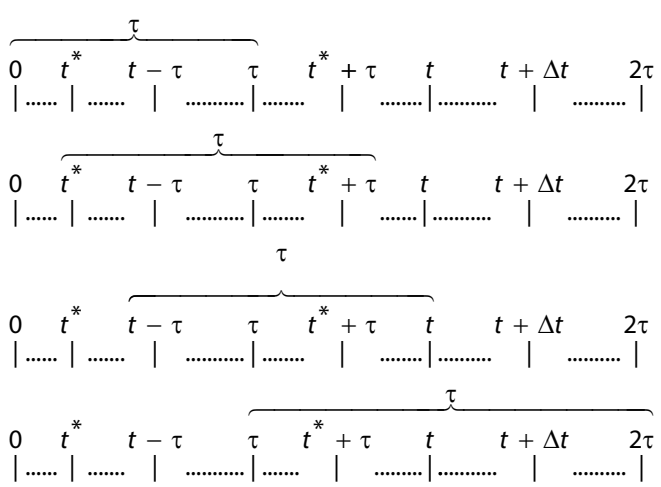

Рис. 3

Рассмотрим всевозможные варианты события $A(0, t + \Delta t)$. Имеем,

$$\begin{aligned}
&A(0,t+\Delta t) = \\
&= B_0^{(0,t-\tau)}B_0^{(t-\tau,t)}B_0^{(t,t+\Delta t)} + B_1^{(0,t-\tau)}B_0^{(t-\tau,t)}B_0^{(t,t+\Delta t)} + \\
&+B_0^{(0,t-\tau)}B_1^{(t-\tau,t)}B_0^{(t,t+\Delta t)} + \\
&+B_1^{(0,t-\tau)}B_0^{(t-\tau,t)}B_1^{(t,t+\Delta t)} + B_0^{(0,t-\tau)}B_0^{(t-\tau,t)}B_1^{(t,t+\Delta t)} + \\
&+ \bigcup_{0<t^*<t-\tau} B_1^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_0^{(t^*+\tau,t)}B_1^{(t,t+\Delta t)} + \\
&+ \bigcup_{0<t^*<t-\tau} B_1^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_1^{(t^*+\tau,t)}B_0^{(t,t+\Delta t)} + \\
&+ \bigcup_{0<t^*<t-\tau} B_0^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_1^{(t^*+\tau,t)}B_0^{(t,t+\Delta t)} + \\
&+ \bigcup_{0<t^*<t-\tau} B_0^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_0^{(t^*+\tau,t)}B_0^{(t,t+\Delta t)} + \\
&+ \bigcup_{0<t^*<t-\tau} B_0^{(0,t^*)}B_1^{(t^*,t^*+\tau)}B_0^{(t^*+\tau,t)}B_0^{(t,t+\Delta t)}.
\end{aligned} \qquad (13)$$

Упростим выражение. Так как справедливы вложения

$$\bigcup_{0<t^*<t-\tau} B_0^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_0^{(t^*+\tau,t)}B_1^{(t,t+\Delta t)} \subset$$
$$\subset B_0^{(0,t-\tau)}B_0^{(t-\tau,t)}B_1^{(t,t+\Delta t)}$$
$$\bigcup_{0<t^*<t-\tau} B_0^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_0^{(t^*+\tau,t)}B_0^{(t,t+\Delta t)} \subset$$
$$\subset B_0^{(0,t-\tau)}B_0^{(t-\tau,t)}B_0^{(t,t+\Delta t)},$$

то, сокращая последнее равенство, имеем

$$\begin{aligned}
&A(0,t+\Delta t) = \\
&= \left[B_0^{(0,t-\tau)}B_0^{(t-\tau,t)} + B_1^{(0,t-\tau)}B_0^{(t-\tau,t)} + B_0^{(0,t-\tau)}B_1^{(t-\tau,t)}\right]B_0^{(t,t+\Delta t)} + \\
&+\left[B_1^{(0,t-\tau)}B_0^{(t-\tau,t)} + B_0^{(0,t-\tau)}B_0^{(t-\tau,t)}\right]B_1^{(t,t+\Delta t)} + \\
&+ \bigcup_{0<t^*<t-\tau} B_1^{(0,t^*)}B_0^{(t^*,t)}B_1^{(t,t+\Delta t)} + \\
&+ \bigcup_{0<t^*<t-\tau} B_1^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_1^{(t^*+\tau,t)}B_0^{(t,t+\Delta t)} + \\
&+ \bigcup_{0<t^*<t-\tau} B_0^{(0,t^*)}B_1^{(t^*,t^*+\tau)}B_0^{(t^*+\tau,t)}B_0^{(t,t+\Delta t)}.
\end{aligned}$$

Заметим, что

$$B_0^{(0,t-\tau)}B_0^{(t-\tau,t)} = B_0^{(0,t)}, B_0^{(t^*+\tau,t)}B_0^{(t,t+\Delta t)} = B_0^{(t^*,t)}.$$

Поэтому, имеем

$$\begin{aligned}
&A(0,t+\Delta t) = \\
&= \left[B_0^{(0,t)} + B_1^{(0,t-\tau)}B_0^{(t-\tau,t)} + B_0^{(0,t-\tau)}B_1^{(t-\tau,t)} + \right. \\
&+ \bigcup_{0<t^*<t-\tau} B_1^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_1^{(t^*+\tau,t)} + \\
&\left. + \bigcup_{0<t^*<t-\tau} B_0^{(0,t^*)}B_1^{(t^*,t^*+\tau)}B_0^{(t^*+\tau,t)}\right]B_0^{(t,t+\Delta t)} + \\
&+\left[B_1^{(0,t-\tau)}B_0^{(t-\tau,t)} + B_0^{(0,t-\tau)}B_0^{(t-\tau,t)} + \right. \\
&\left. + \bigcup_{0<t^*<t-\tau} B_1^{(0,t^*)}B_0^{(t^*,t)}\right]B_1^{(t,t+\Delta t)}.
\end{aligned}$$

Так как

$$B_0^{(t-\tau,t)} \subset B_0^{(t^*,t)},$$

то справедливо равенство

$$\begin{aligned}
&A(0,t+\Delta t) = \\
&= \left[B_0^{(0,t)} + B_1^{(0,t-\tau)}B_0^{(t-\tau,t)} + B_0^{(0,t-\tau)}B_1^{(t-\tau,t)} + \right. \\
&+ \bigcup_{0<t^*<t-\tau} B_1^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_1^{(t^*+\tau,t)} + \\
&\left. + \bigcup_{0<t^*<t-\tau} B_0^{(0,t^*)}B_1^{(t^*,t^*+\tau)}B_0^{(t^*+\tau,t)}\right]B_0^{(t,t+\Delta t)} + \\
&+\left[B_1^{(0,t-\tau)}B_0^{(t-\tau,t)} + B_0^{(0,t-\tau)}B_0^{(t-\tau,t)} + \right. \\
&\left. + \bigcup_{0<t^*<t-\tau} B_1^{(0,t^*)}B_0^{(t^*,t)}B_0^{(t-\tau,t)}\right]B_1^{(t,t+\Delta t)}.
\end{aligned}$$

Далее, упрощая, имеем

$$A(0,t+\Delta t) = \left[B_0^{(0,t)} + B_1^{(0,t-\tau)}B_0^{(t-\tau,t)} + B_0^{(0,t-\tau)}B_1^{(t-\tau,t)} + \bigcup_{0<t^*<t-\tau} B_1^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_1^{(t^*+\tau,t)} + \bigcup_{0<t^*<t-\tau} B_0^{(0,t^*)}B_1^{(t^*,t^*+\tau)}B_0^{(t^*+\tau,t)} \right] B_0^{(t,t+\Delta t)} + \left[B_1^{(0,t-\tau)} + B_0^{(0,t-\tau)} + \bigcup_{0<t^*<t-\tau} B_1^{(0,t^*)}B_0^{(t^*,t)} \right] B_0^{(t-\tau,t)}B_1^{(t,t+\Delta t)}.$$

Поскольку,

$$\bigcup_{0<t^*<t-\tau} B_1^{(0,t^*)}B_0^{(t^*,t)} \subset B_1^{(0,t-\tau)}B_0^{(t-\tau,t)},$$

получим, что

$$A(0,t+\Delta t) = \left[B_0^{(0,t)} + B_1^{(0,t-\tau)}B_0^{(t-\tau,t)} + B_0^{(0,t-\tau)}B_1^{(t-\tau,t)} + \bigcup_{0<t^*<t-\tau} B_1^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_1^{(t^*+\tau,t)} + \bigcup_{0<t^*<t-\tau} B_0^{(0,t^*)}B_1^{(t^*,t^*+\tau)}B_0^{(t^*+\tau,t)} \right] B_0^{(t,t+\Delta t)} + \left[B_1^{(0,t-\tau)} + B_0^{(0,t-\tau)} \right] B_0^{(t-\tau,t)}B_1^{(t,t+\Delta t)}.$$

Так как

$$B_1^{(t^*,t^*+\tau)} = B_1^{(t^*,t-\tau)}B_0^{(t-\tau,t^*+\tau)} + B_0^{(t^*,t-\tau)}B_1^{(t-\tau,t^*+\tau)},$$

то

$$B_0^{(0,t^*)}B_1^{(t^*,t^*+\tau)}B_0^{(t^*+\tau,t)} = B_0^{(0,t^*)}\left(B_1^{(t^*,t-\tau)}B_0^{(t-\tau,t^*+\tau)} + B_1^{(t^*,t-\tau)}B_0^{(t-\tau,t^*+\tau)} \right) B_0^{(t^*+\tau,t)} = B_0^{(0,t^*)}B_1^{(t^*,t-\tau)}B_0^{(t-\tau,t^*+\tau)}B_0^{(t^*+\tau,t)} + B_0^{(0,t^*)}B_0^{(t^*,t-\tau)}B_1^{(t-\tau,t^*+\tau)}B_0^{(t^*+\tau,t)}.$$

Заметим, что

$$B_0^{(0,t^*)}B_0^{(t^*,t-\tau)}B_1^{(t-\tau,t^*+\tau)}B_0^{(t^*+\tau,t)} \subset B_0^{(0,t-\tau)}B_1^{(t-\tau,t)}$$
$$B_0^{(0,t^*)}B_1^{(t^*,t-\tau)}B_0^{(t-\tau,t^*+\tau)}B_0^{(t^*+\tau,t)} \subset B_1^{(0,t-\tau)}B_0^{(t-\tau,t)}.$$

Окончательно, получим

$$A(0,t+\Delta t) = \left[B_0^{(0,t)} + B_1^{(0,t-\tau)}B_0^{(t-\tau,t)} + B_0^{(0,t-\tau)}B_1^{(t-\tau,t)} + \bigcup_{0<t^*<t-\tau} B_1^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_1^{(t^*+\tau,t)} \right] B_0^{(t,t+\Delta t)} + \left[B_1^{(0,t-\tau)} + B_0^{(0,t-\tau)} \right] B_0^{(t-\tau,t)}B_1^{(t,t+\Delta t)}.$$

Так как

$$A(0,t) = B_0^{(0,t)} + B_1^{(0,t-\tau)}B_0^{(t-\tau,t)} + B_0^{(0,t-\tau)}B_1^{(t-\tau,t)} + \bigcup_{0<t^*<t-\tau} B_1^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_1^{(t^*+\tau,t)}$$
$$A(0,t-\tau) = B_1^{(0,t-\tau)} + B_0^{(0,t-\tau)},$$

то получим, что

$$A(0,t+\Delta t) = A(0,t)B_0^{(t,t+\Delta t)} + A(0,t-\tau)B_0^{(t-\tau,t)}B_1^{(t,t+\Delta t)}. \quad (14)$$

Замечание 1. Заметим, что это равенство (14) может быть доказано для любого $t > 0$, так как если все события то момента времени t учтены, то на промежутке времени $t, t+\Delta t$ не должно произойти не одного события. И если все события то момента времени $t-\tau$ учтены, то на промежутке времени $t-\tau, t$ не должно произойти не одного события, но одно событие может произойти на промежутке времени $t, t+\Delta t$.

Заметим, что события $A(0,t)B_0^{(t,t+\Delta t)}$ и $A(0,t-\tau)B_0^{(t-\tau,t)}B_1^{(t,t+\Delta t)}$ несовместимы, так как содержат противоположные события $B_0^{(t,t+\Delta t)}$ и $B_1^{(t,t+\Delta t)}$. Поэтому,

$$P\left(A(0,t+\Delta t)\right) = P\left(A(0,t)B_0^{(t,t+\Delta t)}\right) + P\left(A(0,t-\tau)B_0^{(t-\tau,t)}B_1^{(t,t+\Delta t)}\right). \quad (15)$$

По условию задачи, события $A(0,t)$ и $B_0^{(t,t+\Delta t)}$ независимы. Также независимы события $A(0,t-\tau)$, $B_0^{(t-\tau,t)}$ и $B_1^{(t,t+\Delta t)}$. Поэтому,

$$P\left(A(0,t+\Delta t)\right) = P\left(A(0,t)\right)P\left(B_0^{(t,t+\Delta t)}\right) + P\left(A(0,t-\tau)\right)P\left(B_0^{(t-\tau,t)}\right)P\left(B_1^{(t,t+\Delta t)}\right) = P\left(A(0,t)\right)P\left(B_0^{(0,\Delta t)}\right) + P\left(A(0,t-\tau)\right)P\left(B_0^{(0,\tau)}\right)P\left(B_1^{(0,\Delta t)}\right). \quad (16)$$

Из формулы (16) имеем,

$$\pi(t+\Delta t) = \pi(t)(1-a\Delta t) + \pi(t-\tau)e^{-a\tau}a\Delta t$$
$$\frac{\pi(t+\Delta t)-\pi(t)}{\Delta t} = -a\pi(t) + a\pi(t-\tau)e^{-a\tau},$$

устремляя Δt к нулю получим дифференциальное уравнение

$$\left.\frac{\partial\pi}{\partial t}\right|_{+0} = -a\pi(t) + a\pi(t-\tau)e^{-a\tau}. \quad (17)$$

4. Пусть $\tau < t < 2\tau$ и $\Delta t > 0$, $n \in N$. Обозначим

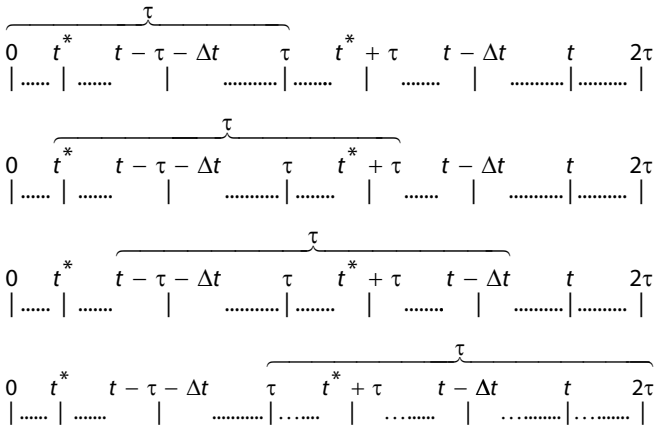

Рис. 4

Рассмотрим всевозможные варианты события $A(0,t+\Delta t)$. Имеем,

$$\begin{aligned}
&A(0,t) = \\
&= B_0^{(0,t-\tau-\Delta t)}B_0^{(t-\tau-\Delta t,t-\Delta t)}B_0(t-\Delta t,t) + \\
&+B_0^{(0,t-\tau-\Delta t)}B_0^{(t-\tau-\Delta t,t-\Delta t)}B_1^{(t-\Delta t,t)} + \\
&+B_0^{(0,t-\tau-\Delta t)}B_1^{(t-\tau-\Delta t,t-\Delta t)}B_0^{(t-\Delta t,t)} + \\
&+B_1^{(0,t-\tau-\Delta t)}B_0^{(t-\tau-\Delta t,t-\Delta t)}B_0^{(t-\Delta t,t)} + \\
&+\bigcup_{0<t^*<t-\tau} B_0^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_0^{(t^*+\tau,t-\Delta t)}B_0^{(t-\Delta t,t)} + \\
&+\bigcup_{0<t^*<t-\tau} B_0^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_0^{(t^*+\tau,t-\Delta t)}B_1^{(t-\Delta t,t)} + \\
&+\bigcup_{0<t^*<t-\tau} B_0^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_1^{(t^*+\tau,t-\Delta t)}B_0^{(t-\Delta t,t)} + \\
&+\bigcup_{0<t^*<t-\tau} B_0^{(0,t^*)}B_1^{(t^*,t^*+\tau)}B_0^{(t^*+\tau,t-\Delta t)}B_1^{(t-\Delta t,t)} + \\
&+\bigcup_{0<t^*<t-\tau} B_1^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_1^{(t^*+\tau,t-\Delta t)}B_0^{(t-\Delta t,t)} + \\
&+\bigcup_{0<t^*<t-\tau} B_0^{(0,t^*)}B_1^{(t^*,t^*+\tau)}B_0^{(t^*+\tau,t-\Delta t)}B_0^{(t-\Delta t,t)}.
\end{aligned} \tag{18}$$

Упростим выражение. Так как справедливы вложения

$$\bigcup_{0<t^*<t-\tau} B_0^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_0^{(t^*+\tau,t-\Delta t)}B_0^{(t-\Delta t,t)} = B_0^{(0,t-\tau-\Delta t)}B_0^{(t-\tau-\Delta t,t-\Delta t)}B_0^{(t-\Delta t,t)}$$

$$\bigcup_{0<t^*<t-\tau} B_0^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_0^{(t^*+\tau,t-\Delta t)}B_1^{(t-\Delta t,t)} = B_0^{(0,t-\tau-\Delta t)}B_0^{(t-\tau-\Delta t,t-\Delta t)}B_1^{(t-\Delta t,t)}$$

$$\bigcup_{0<t^*<t-\tau} B_1^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_0^{(t^*+\tau,t-\Delta t)}B_1^{(t-\Delta t,t)} = B_1^{(0,t-\tau-\Delta t)}B_0^{(t-\tau-\Delta t,t-\Delta t)}B_1^{(t-\Delta t,t)}$$

$$\bigcup_{0<t^*<t-\tau-\Delta t} B_0^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_1^{(t^*+\tau,t-\Delta t)}B_0^{(t-\Delta t,t)} \subset B_0^{(0,t-\tau-\Delta t)}B_1^{(t-\tau-\Delta t,t-\Delta t)}B_0^{(t-\Delta t,t)}.$$

Отсюда следует, что

$$\begin{aligned}
&A(0,t) = \\
&= B_0^{(0,t-\tau-\Delta t)}B_0^{(t-\tau-\Delta t,t-\Delta t)}B_0^{(t-\Delta t,t)} + \\
&+B_0^{(0,t-\tau-\Delta t)}B_0^{(t-\tau-\Delta t,t-\Delta t)}B_1^{(t-\Delta t,t)} + \\
&+B_0^{(0,t-\tau-\Delta t)}B_1^{(t-\tau-\Delta t,t-\Delta t)}B_0^{(t-\Delta t,t)} + \\
&+B_1^{(0,t-\tau-\Delta t)}B_0^{(t-\tau-\Delta t,t-\Delta t)}B_1^{(t-\Delta t,t)} + \\
&+B_1^{(0,t-\tau-\Delta t)}B_0^{(t-\tau-\Delta t,t-\Delta t)}B_0^{(t-\Delta t,t)} + \\
&+\bigcup_{0<t^*<t-\tau-\Delta t} B_1^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_1^{(t^*+\tau,t-\Delta t)}B_0^{(t-\Delta t,t)} + \\
&+\bigcup_{0<t^*<t-\tau-\Delta t} B_0^{(0,t^*)}B_1^{(t^*,t^*+\tau)}B_0^{(t^*+\tau,t-\Delta t)}B_0^{(t-\Delta t,t)}.
\end{aligned}$$

Так как,

$$B_0^{(0,t-\tau-\Delta t)}B_0^{(t-\tau-\Delta t,t-\Delta t)} = B_0^{(0,t-\Delta t)},$$

то

$$\begin{aligned}
&A(0,t) = \\
&= \Big[B_0^{(0,t-\Delta t)} + B_0^{(0,t-\tau-\Delta t)}B_1^{(t-\tau-\Delta t,t-\Delta t)} + \\
&+B_1^{(0,t-\tau-\Delta t)}B_0^{(t-\tau-\Delta t,t-\Delta t)} + \\
&+\bigcup_{0<t^*<t-\tau-\Delta t} B_1^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_1^{(t^*+\tau,t-\Delta t)} + \\
&+\bigcup_{0<t^*<t-\tau-\Delta t} B_0^{(0,t^*)}B_1^{(t^*,t^*+\tau)}B_0^{(t^*+\tau,t-\Delta t)}\Big]B_0^{(t-\Delta t,t)} + \\
&+\Big[B_0^{(0,t-\tau-\Delta t)} + B_1^{(0,t-\tau-\Delta t)}\Big]B_0^{(t-\tau-\Delta t,t-\Delta t)}B_1^{(t-\Delta t,t)}.
\end{aligned}$$

Заметим, что

$$B_1^{(t^*,t^*+\tau)} = B_1^{(t^*,t-\tau-\Delta t)}B_0^{(t-\tau-\Delta t,t^*+\tau)} + B_0^{(t^*,t-\tau-\Delta t)}B_1^{(t-\tau-\Delta t,t^*+\tau)}.$$

Поэтому,

$$\begin{aligned}
&B_0^{(0,t^*)}B_1^{(t^*,t^*+\tau)}B_0^{(t^*+\tau,t-\Delta t)} = \\
&= B_0^{(0,t^*)}\Big(B_1^{(t^*,t-\tau-\Delta t)}B_0^{(t-\tau-\Delta t,t^*+\tau)} + \\
&B_0^{(t^*,t-\tau-\Delta t)}B_1^{(t-\tau-\Delta t,t^*+\tau)}\Big)B_0^{(t^*+\tau,t-\Delta t)} = \\
&= B_0^{(0,t^*)}B_1^{(t^*,t-\tau-\Delta t)}B_0^{(t-\tau-\Delta t,t^*+\tau)}B_0^{(t^*+\tau,t-\Delta t)} + \\
&+B_0^{(0,t^*)}B_0^{(t^*,t-\tau-\Delta t)}B_1^{(t-\tau-\Delta t,t^*+\tau)}B_0^{(t^*+\tau,t-\Delta t)}.
\end{aligned}$$

Из вложения

$$B_0^{(0,t^*)}B_0^{(t^*,t-\tau-\Delta t)}B_1^{(t-\tau-\Delta t,t^*+\tau)}B_0^{(t^*+\tau,t-\Delta t)} \subset$$
$$\subset B_0^{(0,t-\tau-\Delta t)}B_1^{(t-\tau-\Delta t,t-\Delta t)}$$
$$B_0^{(0,t^*)}B_1^{(t^*,t-\tau-\Delta t)}B_0^{(t-\tau-\Delta t,t^*+\tau)}B_0^{(t^*+\tau,t-\Delta t)} \subset$$
$$\subset B_1^{(0,t-\tau-\Delta t)}B_0^{(t-\tau-\Delta t,t-\Delta t)}$$

следует, что

$$A(0,t) =$$
$$= \Big[B_0^{(0,t-\Delta t)} + B_0^{(0,t-\tau-\Delta t)}B_1^{(t-\tau-\Delta t,t-\Delta t)} +$$
$$+B_1^{(0,t-\tau-\Delta t)}B_0^{(t-\tau-\Delta t,t-\Delta t)} +$$
$$+ \bigcup_{0<t^*<t-\tau-\Delta t} B_1^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_1^{(t^*+\tau,t-\Delta t)} \Big] B_0^{(t-\Delta t,t)} +$$
$$+\Big[B_0^{(0,t-\tau-\Delta t)} + B_1^{(0,t-\tau-\Delta t)} \Big] B_0^{(t-\tau-\Delta t,t-\Delta t)}B_1^{(t-\Delta t,t)}.$$

Так как,

$$A(0,t-\Delta t) = B_0^{(0,t-\Delta t)} + B_0^{(0,t-\tau-\Delta t)}B_1^{(t-\tau-\Delta t,t-\Delta t)} +$$
$$+B_1^{(0,t-\tau-\Delta t)}B_0^{(t-\tau-\Delta t,t-\Delta t)} +$$
$$+ \bigcup_{0<t^*<t-\tau-\Delta t} B_1^{(0,t^*)}B_0^{(t^*,t^*+\tau)}B_1^{(t^*+\tau,t-\Delta t)}$$
$$A(0,t-\tau)B_0^{(0,t-\tau-\Delta t)} + B_1^{(0,t-\tau-\Delta t)},$$

то

$$A(0,t) = A(0,t-\Delta t)B_0^{(t-\Delta t,t)} + A(0,t-\tau-\Delta t)B_0^{(t-\tau-\Delta t,t-\Delta t)}B_1^{(t-\Delta t,t)}. \quad (19)$$

Замечание 2. Заметим, что это равенство может быть доказано для любого $t > 0$, так как если все события то момента времени $t-\Delta t$ учтены, то на промежутке времени $t-\Delta t, t$ не должно произойти не одного события. И если все события до момента времени $t-\tau-\Delta t$ учтены, то на промежутке времени $t-\tau-\Delta t, t-\Delta t$ не должно произойти не одного события, но одно событие может произойти на промежутке времени $t-\Delta t, t$.

Поэтому, из формулы (19) имеем,

$$\pi(t) = \pi(t-\Delta t)(1-a\Delta t) + \pi(t-\tau-\Delta t)e^{-a\tau}a\Delta t$$
$$\frac{\pi(t-\Delta t)-\pi(t)}{-\Delta t} = -a\pi(t-\Delta t) + a\pi(t-\tau-\Delta t)e^{-a\tau},$$

устремляя Δt к нулю получим дифференциальное уравнение

$$\left.\frac{\partial\pi}{\partial t}\right|_{-0} = -a\pi(t) + a\pi(t-\tau)e^{-a\tau}. \quad (20)$$

Объединяя равенства (17) и (20) получим уравнение

$$\frac{\partial\pi}{\partial t} = -a\pi(t) + a\pi(t-\tau)e^{-a\tau} \quad (21)$$

с начальным условием

$$\pi(\tau) = e^{-a\tau}(1+a\tau). \quad (22)$$

Замечание 3. Заметим, что уравнение (21) справедливо для всех $t > \tau$.

Так как $0 < t-\tau < \tau$, то подставляя вместо $\pi(t-\tau)$ выражение (12) в последнее дифференциальное уравнение, получим уравнение

$$\frac{\partial\pi}{\partial t} = -a\pi(t) + ae^{-a(t-\tau)}\big(1+a(t-\tau)\big)e^{-a\tau} = \quad (23)$$
$$= -a\pi(t) + ae^{-a\tau}\big(1+a(t-\tau)\big)$$

с начальным условием (22).

Решением уравнения (23) при условии (22) будет функция

$$\pi(t) = \exp(-at)\left(1 + at + \frac{a^2(t-\tau)^2}{2!}\right). \quad (24)$$

5. Пользуясь методом математической индукции, покажем, что для $(n-1)\tau < t \le n\tau$ решение уравнения (21) имеет вид

$$\pi(t) = \exp(-at)\sum_{k=1}^{k=n}\frac{a^k\big[t-(k-1)\tau\big]^k}{k!}. \quad (25)$$

Пусть $(n-2)\tau < t \le (n-1)\tau$ и решение уравнения (21) имеет вид

$$\pi(t) = \exp(-at)\sum_{k=1}^{k=n-1}\frac{a^k\big[t-(k-1)\tau\big]^k}{k!}. \quad (26)$$

В этом случае при $(n-1)\tau < t \le n\tau$, согласно замечанию 3 аналогично доказывается уравнение (21). Подставляя в уравнение (21) выражение (26), получим уравнение

$$\frac{\partial\pi}{\partial t} = -a\pi(t) + a\pi(t-\tau)\exp(-a\tau) = -a\pi(t) +$$
$$+a\exp\big(-a(t-\tau)\big)\sum_{k=1}^{k=n-1}\frac{a^k\big[t-\tau-(k-1)\tau\big]^k}{k!}\exp(-a\tau) = \quad (27)$$
$$= -a\pi(t) + a\exp(-at)\sum_{k=1}^{k=n-1}\frac{a^k[t-k\tau]^k}{k!}.$$

Начальное условие определим равенством

$$\pi\big((n-1)\tau\big) =$$
$$= \exp\big(-a(n-1)\tau\big)\sum_{k=1}^{k=n-1}\frac{a^k\big[(n-1)\tau-(k-1)\tau\big]^k}{k!} = \quad (28)$$
$$= \exp\big(-a(n-1)\tau\big)\sum_{k=1}^{k=n-1}\frac{a^k\big[(n-k)\tau\big]^k}{k!}.$$

Покажем, что функция (25) будет решением уравнения (27) на отрезке $(n-1)\tau < t \le n\tau$ при начальных условиях (28). Имеем

$$\pi^*(t) = \left(\exp(-at)\sum_{k=1}^{k=n}\frac{a^k\left[t-(k-1)\tau\right]^k}{k!}\right)^* =$$

$$= -a\exp(-at)\sum_{k=0}^{k=n}\frac{a^k\left[t-(k-1)\tau\right]^k}{k!} +$$

$$+a\exp(-at)\sum_{k=1}^{k=n}\frac{ka^{k-1}\left[t-(k-1)\tau\right]^{k-1}}{(k-1)!k} =$$

$$= -a\exp(-at)\sum_{k=0}^{k=n}\frac{a^k\left[t-(k-1)\tau\right]^k}{k!} +$$

$$+a\exp(-at)\sum_{k=0}^{k=n-1}\frac{a^k\left[t-k\tau\right]^k}{k!}$$

и подставляя в (25) условие $t = (n-1)\tau$ имеем

$$\pi\left((n-1)\tau\right) =$$

$$= \exp\left(-a(n-1)\tau\right)\sum_{k=1}^{k=n}\frac{a^k\left[(n-1)\tau-(k-1)\tau\right]^k}{k!}$$

$$= \exp\left(-a(n-1)\tau\right)\sum_{k=1}^{k=n-1}\frac{a^k\left[(n-k)\tau\right]^k}{k!},$$

что совпадает с (28).

Так как для любого $t \in R$ существует единственный $n \in N$, такой что $\tau(n-1) < t \le \tau n$, то можно ввести функцию, не зависящую от n. Обозначим

$$\psi(t) = \begin{cases}\left[\frac{t}{\tau}\right]+1, & \tau(n-1) < t < \tau n\\ \left[\frac{t}{\tau}\right], & t = \tau n\end{cases},$$

где $[x]$ — целая часть числа x. Поэтому, равенство (25) для всех $t > 0$ можно переписать в виде

$$P\left(A(0,t)\right) = \pi(t) = \exp(-at)\sum_{k=1}^{\psi(t)}\frac{a^k\left(t-(k-1)\tau\right)^k}{k!}, \quad (29)$$

которое уже справедливо для всех $t > \tau$.

Заключение

Итак, выбирая некоторое $t > 0$ (в зависимости от эффективности работы антивирусной программы необходимой нам для оценивания больших или малых промежутков времени), число $a = -\ln\left(P(0,1)\right)$ из статистических выводов (самый простой — провести n экспериментов прихода вредоносных программ на единичном интервале и разделить количество неудачных экспериментов (за время $[0,1]$ появилось хоть одно вредоносное воздействие) по общее число экспериментов n, получим приблизительно $P(0,1)$, можно с некоторой точностью) и τ — как среднее время обработки вредоносного воздействия (взятое из характеристик антивирусной программы), сравнивая несколько антивирусных программ, можно выбрать наилучшую (для которой величина (29) максимальная).

Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финуниверситета.

ЛИТЕРАТУРА

1. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты»
2. Гнеденко Б.В. Курс теории вероятностей / Б.В. Гнеденко. — Москва: Издательство «УРСС», 2001.
3. Венцель Е.С. Теория случайных процессов и ее инженерные приложения / Е.С. Венцель, Л.А. Очаров. — Москва: Издательство «Высшая школа», 2000.
4. Венцель Е.С. Теория вероятностей и ее инженерные приложения / Е.С. Венцель, Л.А. Очаров. — Москва: Издательство «Высшая школа», 2000.
5. Вероятностные процессы /Дуб Дж. Л. // М. ИЛ, 1956
6. Теория вероятностей и Марковские процессы / Дынкин Е.Б., Юшкевич А.А. // Физматгиз, 1966