МОДЕЛЬ ОЦЕНИВАНИЯ ОПЕРАТИВНОСТИ УСТРАНЕНИЯ ВРЕДОНОСНЫХ ВОЗДЕЙСТВИЙ НА СЕТЬ ПЕРЕДАЧИ ДАННЫХ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Л.М. Груздева (Москва)

Необходимым условием эффективности функционирования корпоративных сетей передачи данных (КСПД) является обеспечение требуемого уровня защиты информации от вредоносных воздействий [1, 2], который может быть достигнут внедрением системы защиты информации (СЗИ) [3], реализующей различные технологии по обнаружению и противодействию кибератакам с использованием вредоносного программного обеспечения (ВПО), как самого распространенного, по данным аналитических отчетов компании Positive Technologies, метода атак злоумышленников (рис. 1).

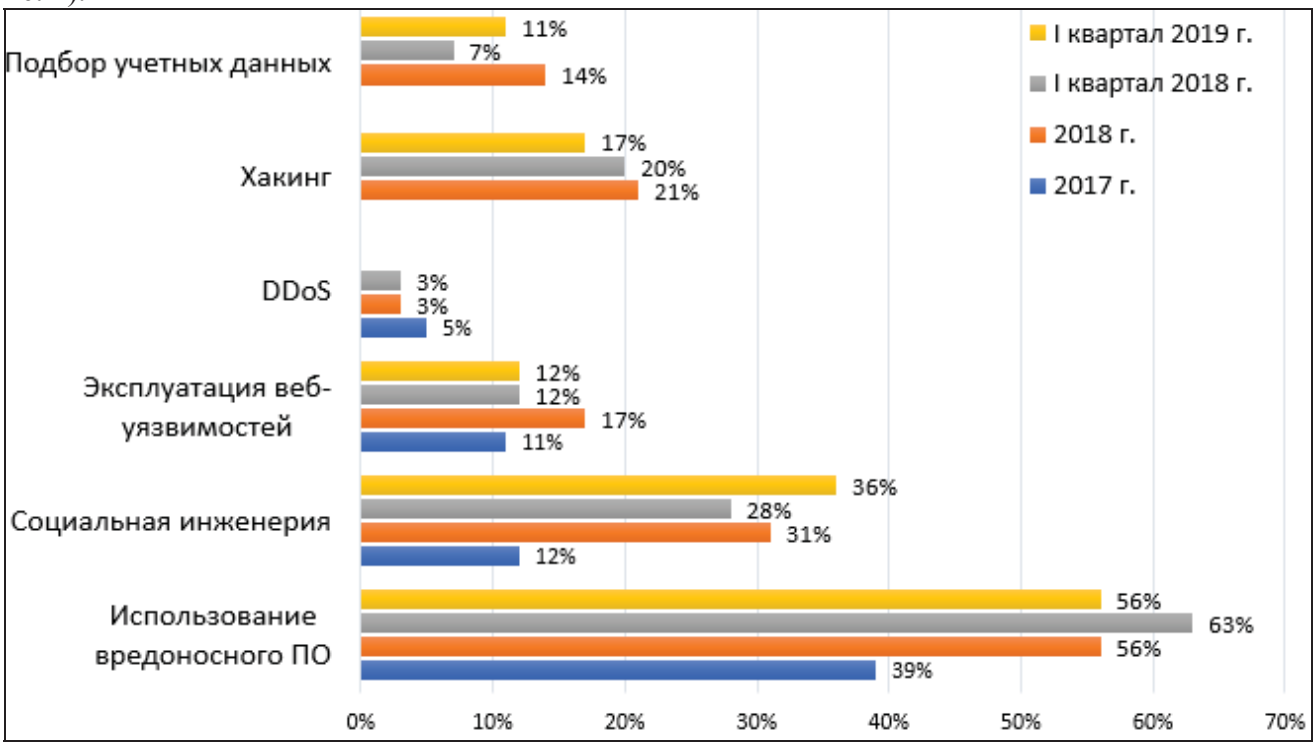

Рис. 1. Методы атак

С 2018 г. наиболее популярным стало программное обеспечение для шпионажа, с помощью которого злоумышленники собирают конфиденциальную информацию как юридических, так и частных лиц, или, в случае целенаправленной атаки, закрепляются в системе (рис. 2).

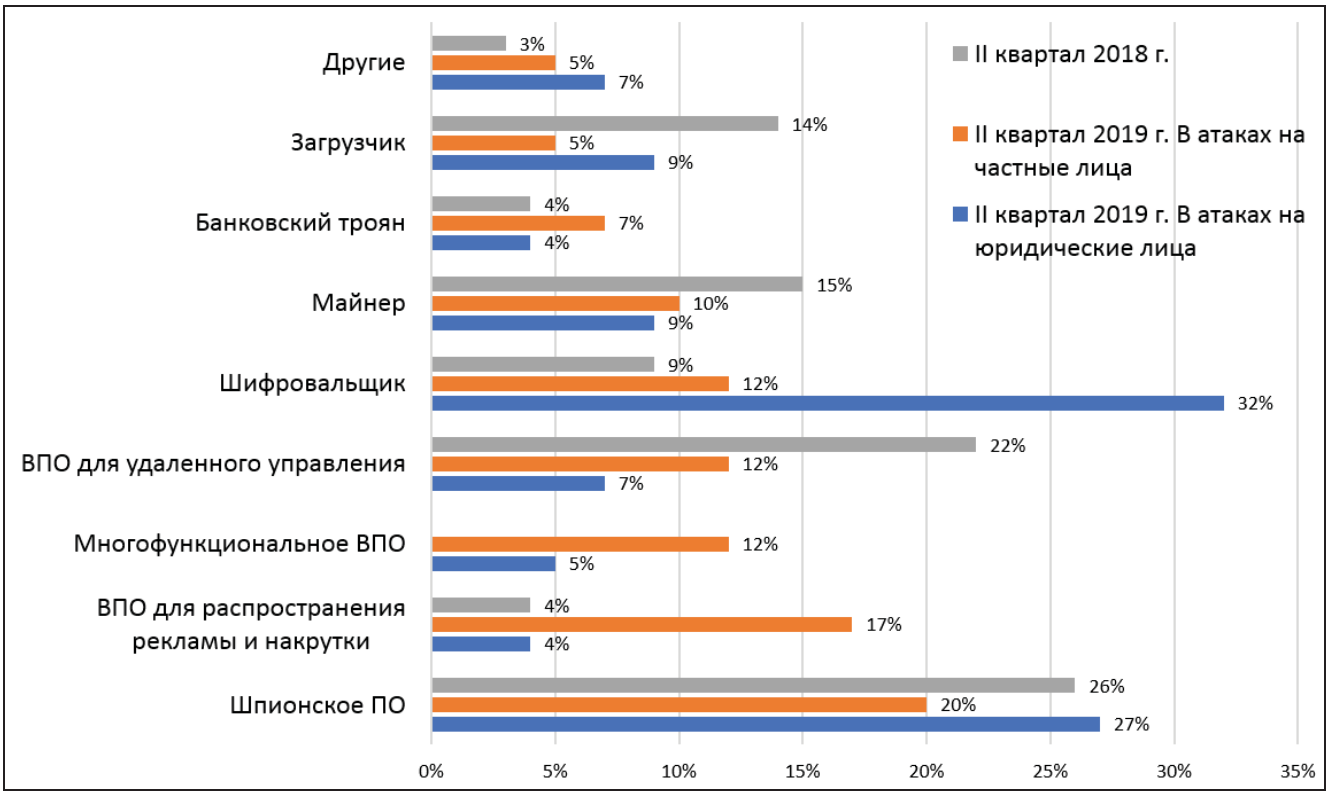

Рис. 2. Типы вредоносного программного обеспечения

Постановка задачи. Разработать математическую модель процесса устранения вредоносных воздействий, использование которой обеспечит возможность оценки качества работы СЗИ и функционирования КСПД в различные моменты времени в зависимости от начального числа вредоносных воздействий (вредоносных программ), используемых методов обнаружения и противодействия.

Под вредоносным воздействием будем понимать распространение вредоносных программ в КСПД, любые их действия, которые могут привести к нарушению работоспособности, как отдельных узлов, так и сети в целом.

Математическая модель. Пусть КСПД состоит из множества узлов (компьютерных систем, КС - S), в каждом из которых протекает случайный процесс распространения (действий) вредоносных программ. Система S может находиться в одном из дискретных состояний: s_0, s_1,…, s_N, где N – количество вредоносных воздействий (как частный случай, Nможет быть равно числу вредоносных программ в узле сети). Пусть процесс обнаружения вредоносных воздействий связан с переходом системы S из одного состояния в другое. Предположим, что этот процесс является марковским [4, 5] и имеет одно поглощающее состояние – s_0. Интенсивность обнаружения вредоносных воздействий или вредоносных программ будем считать пропорциональным их числу. Предположим также, что обнаруженное вредоносное воздействие мгновенно устраняется. Скорость обнаружения вредоносных воздействий измеряется временем обнаружения одного вредоносного воздействия, которое является случайной величиной с известным распределением.

Пусть в начальный момент времени в S содержится N вредоносных воздействий. Эффективность каждого сканирования системы S определяется величиной p_{ij} – вероятностью того, что после сканирования в КС, содержащей $i(i = \overline{0,N})$ вредоносных воздействий, останутся необнаруженными j ($j \geq i$ или $j<i$), $(j = \overline{0,N})$. Распределение p_{ij} задается в виде квадратной матрицы размером $(N+1)\times(N+1)$:

$$P = \begin{Vmatrix} p_{N,N} & p_{N,N-1} & p_{N,N-2} & \cdots & p_{N,j} & \cdots & p_{N,1} & p_{N,0} \\ p_{N-1,N} & p_{N-1,N-1} & p_{N-1,N-2} & \cdots & p_{N-1,j} & \cdots & p_{N-1,1} & p_{N-1,0} \\ p_{i,N} & p_{i,N-1} & p_{i,N-2} & \cdots & p_{i,j} & \cdots & p_{i,1} & p_{i,0} \\ p_{1,N} & p_{1,N-1} & p_{1,N-2} & \cdots & p_{1,j} & \cdots & p_{1,1} & p_{1,0} \\ 0 & 0 & 0 & \dots & 0 & \dots & 0 & 1 \end{Vmatrix} \quad (1)$$

Представим матрицу (1) посредством эквивалентных преобразований в канонической форме: $P = \begin{Vmatrix} I & O \\ R & Q \end{Vmatrix}$ (2), где I – единичная матрица; O – нулевой вектор-строка длиной N; R – вектор-столбец длиной N: $R = \begin{Vmatrix} p_{N,0} \\ p_{N-1,0} \\ \vdots \\ p_{1,0} \end{Vmatrix}$; Q – квадратная подматрица переходов: $Q = \begin{Vmatrix} p_{N,N} & p_{N,N-1} & \cdots & p_{N,1} \\ p_{N-1,N} & p_{N-1,N-1} & \cdots & p_{N-1,1} \\ p_{1,N} & p_{1,N-1} & \cdots & p_{1,1} \end{Vmatrix}$.

Пусть время поиска вредоносного воздействия равно одной условной временной единице. Поставим в соответствие i-му $(i = \overline{0,N})$ числу вредоносных воздействий в КС i-е состояние марковского процесса. Тогда процесс устранения вредоносного воздействия будет представлять собой случайное блуждание точки в пространстве $N+1$ состояний.

При предположении, что в КС во время поиска не может быть больше N вредоносных воздействий и уже устраненные не могут вновь появиться в данной системе, процесс поиска и устранения можно представить в виде модели случайных блужданий с конечным числом состояний, с отражающим и поглощающим экранами. На основе использования данной модели определим важные временные и вероятностные характеристики процесса поиска и устранения вредоносных воздействий, необходимые при планировании данных процессов.

Процесс устранения вредоносных воздействий обычно может происходить в условиях ограниченного времени (ресурсов) и при отсутствии таких ограничений. Анализ характеристик в условиях отсутствия ограничений позволяет также получить предельные значения требуемых характеристик устранения вредоносных воздействий.

Методы и средства исследований. Анализ предложенной модели позволил сделать вывод, что наиболее важными характеристиками процесса поиска и устранения вредоносных воздействий являются [6]:

1) математическое ожидание времени, в течение которого в компьютерной системе находится j вредоносных воздействий, при условии, что в начале поиска их было i [элементы $M_i(n_j)$ матрицы N]:

$N = (I - Q)^{-1}$ (при неограниченном времени);

$N(n) = 1 + Q + Q^2 + \ldots + Q^n$, где n – количество циклов поиска (при ограниченном времени);

$$N = \begin{Vmatrix} \frac{1}{f(N,p_{1,0})} & \frac{1}{f(N-1,p_{1,0})} & \cdots & \frac{1}{f(1,p_{1,0})} \\ 0 & \frac{1}{f(N-1,p_{1,0})} & \cdots & \frac{1}{f(1,p_{1,0})} \\ 0 & 0 & \dots & \frac{1}{f(1,p_{1,0})} \end{Vmatrix}, \quad f(i,p_{1,0}) = p_{i,i-1}$$ - вероятность того, что после одного сканирования в компьютерной системе будет i-1 вредоносных воздействий, при условии, что до этого в ней было i вредоносных воздействий (при последовательном устранении в режиме неограниченного времени).

2) дисперсия времени, в течение которого в компьютерной системе находится j вредоносных воздействий, при условии, что в начале поиска их было i [элементы $D_i(n_j)$ матрицы N_2]:

$N_2 = N(2N_{dg} - I) - N_{sq}$, где N_{dg} – матрица, на главной диагонали которой стоят соответствующие элементы матрицы N, а на остальных нули; N_{sq}– матрица, полученная из N возведением в квадрат каждого ее элемента (при неограниченном времени);

$$N = \left\| \begin{matrix} \left(\frac{1}{f^2(N,p_{1,0})} - \frac{1}{f(N,p_{1,0})}\right) & \dots & \left(\frac{1}{f^2(1,p_{1,0})} - \frac{1}{f(1,p_{1,0})}\right) \\ 0 & \dots & \left(\frac{1}{f^2(1,p_{1,0})} - \frac{1}{f(1,p_{1,0})}\right) \\ 0 & \dots & \left(\frac{1}{f^2(1,p_{1,0})} - \frac{1}{f(1,p_{1,0})}\right) \end{matrix} \right\|$$

(при последовательном устранении в режиме неограниченного времени).

3) математическое ожидание времени устранения всех вредоносных воздействий в компьютерной системе при условии, что в начале поиска в компьютерной системе было *i* вредоносных воздействий [элементы $M_i(n_0)$ матрицы τ]:

$\tau = N\xi$, где ξ - единичный вектор-столбец (при неограниченном времени);

$\tau(n) = N(n)\xi$ (при ограниченном времени);

$$\tau = \left\| \begin{matrix} \sum_{i=1}^{N} \frac{1}{f(i,p_{1,0})} \\ \sum_{i=1}^{N-1} \frac{1}{f(i,p_{1,0})} \\ \sum_{i=1}^{1} \frac{1}{f(i,p_{1,0})} \end{matrix} \right\|$$

(при последовательном устранении в режиме неограниченного времени).

4) дисперсия времени устранения всех вредоносных воздействий в компьютерной системе при условии, что в начале поиска в компьютерной системе было *i* вредоносных воздействий [элементы $D_i(n_0)$ матрицы τ_2]:

$\tau_2 = (2N - I)\tau - \tau_{sq}$, где τ_{sq} – вектор-столбец, полученный из вектора-столбца τ возведением в квадрат каждого его элемента (при неограниченном времени);

$$\tau_2 = \left\| \begin{matrix} \left(\frac{2}{f(N,p_{1,0})} - 1\right)\left(\sum_{i=1}^{N} \frac{1}{f(i,p_{1,0})}\right) + \dots \\ \dots + \left(\frac{2\cdot 1}{f(1,p_{1,0})f(1,p_{1,0})} - 1\right) - \left(\sum_{i=1}^{N} \frac{1}{f(i,p_{1,0})}\right)^2 \\ \left(\frac{2}{f(N-1,p_{1,0})} - 1\right)\left(\sum_{i=1}^{N-1} \frac{1}{f(i,p_{1,0})}\right) + \dots \\ \dots + \left(\frac{2\cdot 1}{f(1,p_{1,0})f(1,p_{1,0})}\right) - \left(\sum_{i=1}^{N-1} \frac{1}{f(i,p_{1,0})}\right)^2 \\ \dots\dots\dots\dots\dots\dots \\ \left(\frac{2\cdot 1}{f(1,p_{1,0})} - 1\right)\left(\frac{1}{f(1,p_{1,0})}\right) - \left(\frac{1}{f(1,p_{1,0})}\right)^2 \end{matrix} \right\|$$

(при последовательном устранении в режиме неограниченного времени).

5) вероятность устранения всех вредоносных воздействий в компьютерной системе при условии, что в начале поиска в компьютерной системе было *i* вредоносных программ:

$B = NR$ (при неограниченном времени);

$B(n) = R + QR + \dots + Q^{n-1}R$ (при ограниченном времени);

$$B = \left\| \begin{matrix} 1 \\ 1 \\ \dots \\ 1 \end{matrix} \right\|$$

(при последовательном устранении в режиме неограниченного времени).

6) математическое ожидание времени, в течение которого в компьютерной системе существует постоянное число вредоносных воздействий, при условии, что в начале их было *i* [элементы $M_i(r_i)$ матрицы M]:

$M_i[r_i] = \frac{1}{1-p_{ii}}$ (при неограниченном времени);

$M_i[r_i(n)] = \frac{1-p_{ii}^{n+1}}{1-p_{ii}}$ (при ограниченном времени);

$\{M_i[r_i]\} = \left\| \begin{matrix} \frac{1}{f(N,p_{1,0})} \\ \frac{1}{f(N-1,p_{1,0})} \\ \cdots \\ \frac{1}{f(1,p_{1,0})} \end{matrix} \right\|$ (при последовательном устранении в режиме неограниченного времени).

7) дисперсия времени, в течение которого в компьютерной системе существует постоянное число вредоносных воздействий, при условии, что в начале их было *i*:

$D_i[r_i] = \frac{p_{ii}}{(1-p_{ii})^2}$ (при неограниченном времени);

$\{D_i[r_i]\} = \left\| \begin{matrix} \frac{1-f(N,p_{1,0})}{f(N,p_{1,0})} \\ \frac{1-f(N-1,p_{1,0})}{f(N-1,p_{1,0})} \\ \cdots \\ \frac{1-f(1,p_{1,0})}{f(1,p_{1,0})} \end{matrix} \right\|$ (при последовательном устранении в режиме неограниченного времени).

8) вероятность того, что в компьютерной системе находится j вредоносных воздействий, при условии, что в начале поиска их было i [элементы h_{ij}матрицы H]:

$H = (N-I)N_{dg}^{-1}$ (при неограниченном времени);

$h_{i_j}(n) = 1 - \prod_{\mu=1}^{n}\left(1 - p_{ij}^{\mu}\right)$, где $h_{i_j}(n)$ – элементы матрицы H(n) (при ограниченном времени);

$H = \left\| \begin{matrix} 1 - f(N,p_{1,0}) & 1 & \dots & 1 \\ 0 & 1 - f(N-1,p_{1,0}) & \dots & 1 \\ 0 & 0 & \dots & 1 - f(1,p_{1,0}) \end{matrix} \right\|$ (при последовательном устранении в режиме неограниченного времени).

9) вероятность того, что в процессе поиска в компьютерной системе j вредоносных воздействий встретится ровно k раз, при условии, что в начале поиска их было i [элементы h_{ij}^{*} матрицы $H^{(k)}$]:

$H^{(k)} = \begin{cases} E - H, \text{если} k = 0 \\ \text{НН}_{\text{dg}}^{\text{k-1}} \times \left[I - H_{dg}\right], \\ \text{если} k \neq 0 \end{cases}$ где H_{dg} – матрица, на главной диагонали которой стоят соответствующие элементы матрицы H, а на остальных нули (при неограниченном времени);

$H_{(n)}^{(k)} = \begin{cases} E - H, \text{если} k = 0 \\ H(n)H_{\text{dg}}^{\text{k-1}}(n) \times \left[I - H_{dg}(n)\right]; \\ 0 < k \leq n, \\ \text{если} k \neq 0 \end{cases}$ (при ограниченном времени);

$E_{k=0} - H = \left\| \begin{matrix} f(N,p_{1,0}) & \dots & 0 \\ 0 & \dots & f(1,p_{1,0}) \end{matrix} \right\|,$

$H_{k\neq 0}^{(k)} = \left\| \begin{matrix} \left[(1 - f(N,p_{1,0})^k f(N,p_{1,0})\right] & \dots & 0 \\ 0 & \dots & \left[(1 - f(1,p_{1,0})^k f(1,p_{1,0})\right] \end{matrix} \right\|$ (при последовательном устранении в режиме неограниченного времени).

10) среднее число вредоносных воздействий в компьютерной системе за время поиска при условии, что в начале поиска в ней было i вредоносных воздействий:

$\mu = \left[H + \left(I - H_{dg}\right)\right]\xi$ (при неограниченном времени);

$\mu = \left[H(n) + \left(I - H_{dg}(n)\right)\right]\xi$ (при ограниченном времени);

$\mu = \begin{Vmatrix} N \\ N-1 \\ N-2 \\ 1 \end{Vmatrix}$ (при последовательном устранении в режиме неограниченного времени).

Для оценки некоторых характеристик СЗИ было проведено имитационное моделирование процесса поиска и устранения вредоносных воздействий.

Исходной для функционирования имитационной модели информацией являлись матрица переходов $Q = \begin{Vmatrix} 0.13 & 0.10 & 0.20 & 0.00 & 0.20 \\ 0.20 & 0.15 & 0.05 & 0.20 & 0.15 \\ 0.20 & 0.00 & 0.00 & 0.30 & 0.00 \\ 0.26 & 0.00 & 0.24 & 0.00 & 0.10 \\ 0.27 & 0.20 & 0.00 & 0.23 & 0.30 \end{Vmatrix}$ и начальное число вредоносных воздействий, обнаруженных в каждом узле сети, заданное вектором-строкой $A = (3 \quad 5 \quad 8 \quad 4 \quad 2)$. Элементы матрицы Q- вероятности того, что вредоносное воздействие, обнаруженное в одном модуле сети, вызывает процесс поиска и устранения в другом.

Общее число процессов поиска и устранения вредоносных воздействий, которые необходимо запустить во всех модулях сети, определенное с помощью предложенной модели, равно

$$N = \left|\begin{matrix} 4.766 & 0.962 & 1.230 & 0.953 & 1.704 \\ 3.681 & 7.003 & 1.707 & 2.585 & 2.922 \\ 4.074 & 0.918 & 9.707 & 3.524 & 1.864 \\ 2.554 & 0.675 & 1.751 & 5.027 & 1.593 \\ 2.066 & 1.159 & 0.799 & 1.366 & 3.891 \end{matrix}\right| \begin{matrix} 9.615 \\ 17.898 \\ 20.087 \\ 11.600 \\ \underbrace{9.281}_{68.481} \end{matrix}$$

и целая часть этого числа есть искомая оценка (68). Для оценки времени, необходимого СЗИ, можно воспользоваться формулой *T=N/C*, где *C*– постоянная скорость поиска и устранения вредоносных воздействий.

Заключение.Оценка эффективности систем защиты информации в корпоративных сетях передачи данных от вредоносных воздействий, требует разработки математической модели процесса устранения данных воздействий в сети. Распространение вредоносных программ, с помощью которых злоумышленники реализуют угрозы на информационные ресурсы компьютерных сетей, следует рассматривать как вредоносное воздействие. Причиной успешных атак на информационные ресурсы следует считать неэффективную организацию защитных механизмов корпоративных сетей, не обеспечивающую требуемый уровень противодействия вредоносным воздействиям.

Для оценки характеристик трудоемкости устранения вредоносных воздействий в КСПД разработана математическая модель. На основе предложенной модели возможна оценка наиболее важных характеристик процесса устранения вредоносных воздействий (вредоносных программ) в сети: математическое ожидание и дисперсия времени поиска вредоносных воздействий; математическое ожидание и дисперсия времени устранения всех вредоносных воздействий; вероятность устранения всех вредоносных воздействий; среднее число вредоносных воздействий в компьютерной системе за время поиска.

Литература

1. Груздева Л.М. Повышение производительности корпоративной сети АСУ в условиях воздействия угроз информационной безопасности / Л.М. Груздева, М.Ю. Монахов // Известия высших учебных заведений. Приборостроение. – 2012. – Т. 55. – № 8. – С.53-56.

2. Монахов, Ю.М. Теоретическое и экспериментальное исследование распределенных телекоммуникационных систем в условиях воздействия вредоносных программ: монография / Ю. М. Монахов, Л. М. Груздева; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир: Изд-во ВлГУ, 2013. – 132 с.

3. Методы и модели оценки инфраструктуры системы защиты информации в корпоративных сетях промышленных предприятий: монография / под ред. П.П. Парамонова. – СПб: Изд-во ООО «Студия «НП-Принт», 2012. – 115 с.
4. Клейнрок Л. Теория массового обслуживания / Л. Клейнрок. – М.: Книга по Требованию, 2013. – 429 с.
5. Вентцель Е.С. Теория случайных процессов и ее инженерные приложения: учебное пособие / Е. С. Вентцель, Л. А. Овчаров. – 5-е изд., стер. – М.: КноРус, 2016. – 448 с.
6. Мамиконов А.Г. Достоверность, защита и резервирование информации в АСУ / А.Г. Мамиконов, В.В. Кульба, А.Б. Шелков. – М.: Энергоатомиздат, 1986. – 304 с.