М. М. Тараскин, В. Д. Денисенко

ПОДХОД К ОЦЕНКЕ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Локальная вычислительная сеть (ЛВС) представляет взаимосвязанные и взаимодействующие между собой элементы, которые могут функционировать в условиях воздействия негативных факторов, в частности компьютерных атак (КА).

Основными пользовательскими свойствами ЛВС являются виды и уровни услуг, оказываемых потребителям. Наряду с информационным обменом в ЛВС существует контроль качества обмена информацией, алгоритмами работы и параметрами, который характеризуется такими основными свойствами, как оперативность, точность, доступность, отказоустойчивость и т. п. Оценка эффективности ЛВС в условиях противоречивости показателей ее функционирования представляет научно-практический интерес и является предметом исследований.

Показатели эффективности ЛВС могут быть разделены на внешние и внутренние [1]. Внешние показатели тождественны системе показателей процессов приема, обработки, передачи данных и используются для оценки эффективности ЛВС. Внутренние показатели характеризуют эффективность различных компонентов ЛВС, например системы обнаружения вторжений, системы антивирусной защиты и т. п.

Следовательно, интерес для исследований представляют как внешние, так и внутренние показатели, определяющие качество функционирования ЛВС, а также зависимости между показателями.

Введение перечисленных внешних и внутренних показателей, их аналитическое представление и установление зависимостей между ними позволят оценивать эффективность подходов, направленных на совершенствование процесса обнаружения КА в локальных вычислительных сетях.

Эффективность функционирования ЛВС в условиях воздействия КА может быть оценена:

$$ЭФ(t) = P_{\text{с.}}(t) \times P_{\text{д.}}(t) \times P_{\text{защ.}}(t) \times \left(1 - K_{\text{зат.}}\right), \quad (1)$$

где $ЭФ(t)$ — показатель эффективности функционирования ЛВС в условиях воздействия КА; $P_{\text{с.}}(t)$ — вероятность своевременного выполнения какой-либо услуги; $P_{\text{д}}(t)$ — вероятность достоверного выполнения какой-либо услуги; $P_{\text{защ.}}(t)$ — вероятность защищенности выполнения какой-либо услуги; $K_{\text{зат.}}$ — коэффициент затрат.

В выражении (1) $ЭФ(t)$ изменяется в зависимости от времени; в фиксированный момент времени $ЭФ(t)$ имеет определенное числовое значение. Коэффициент затрат ($K_{\text{зат.}}$) — безразмерная величина (изменяющаяся в пределах от 0 до 1), вычисляемая посредством отнесения величины реальных затрат к величине допустимых затрат.

Внешний показатель — вероятность защищенности выполнения какой-либо услуги в условиях воздействия КА:

$$\rho_{\text{защ.}}(t) = \rho_{\text{обн.КА}}(t_{\text{обн.КА}} \le T_{\text{обн.тр.}}) \times \rho_{\text{НСВ}}(t_{\text{НСВ}} \ge t_{\text{НСВтр.}}) \times \rho_{\text{НСД}}(t_{\text{НСД}} \ge t_{\text{НСДтр.}}), \quad (2)$$

где $\rho_{\text{обн.КА}}(t_{\text{обн.КА}} \le T_{\text{обн.тр.}})$ — вероятность обнаружения КА (вероятность такого события, при котором время обнаружения КА не превышает требуемое); $\rho_{\text{НСВ}}(t_{\text{НСВ}} \ge t_{\text{НСВтр.}})$ — вероятность защищенности от несанкционированного воздействия (НСВ) (вероятность такого события, при котором время, необходимое нарушителю для осуществления воздействия, будет более требуемого); $\rho_{\text{НСД}}(t_{\text{НСД}} \ge t_{\text{НСДтр.}})$ — вероятность защищенности от несанкционированного доступа (НСД) (вероятность такого события, при котором время, необходимое нарушителю для осуществления НСД, будет более требуемого).

В выражении (2) в качестве аргумента функции $P_{\text{защ.}}(t)$ выступают $t_{\text{обн.КА}}$ — время обнаружения КА, $t_{\text{НСВ}}$ — время несанкционированного воздействия, $t_{\text{НСД}}$ — время несанкционированного доступа, однако в статье рассматривается поведение только $t_{\text{обн.КА}}$.

Внутренний показатель — вероятность обнаружения КА [1]:

$$P_{\text{обн. КА}}(t) = P_{\text{св.обн. КА}}(t) \times P_{\text{дост. обн. КА}}(t), \tag{3}$$

где $P_{\text{св.обн.КА}}(t)$ — вероятность своевременного обнаружения КА; $P_{\text{дост.обн.КА}}(t)$ — вероятность достоверного обнаружения КА.

$$P_{\text{св.обн. КА}}(t) = P_{\text{св. обн. стр.}}(t) \times P_{\text{св. обн. стат.}}(t), \tag{4}$$

где $P_{\text{св.обн.стр.}}(t)$ — вероятность своевременного обнаружения КА по структурным признакам; $P_{\text{св.обн.стат.}}(t)$ — вероятность своевременного обнаружения КА по статистическим признакам.

$$P_{\text{св.обн. стр.}}(t) = 1 - e^{\left(-\frac{T_{\text{обн. тр.}}}{t_{\text{обн. стр.}}}\right)}, \tag{5}$$

где $T_{\text{обн.тр.}}$ — требуемое время обнаружения КА; $T_{\text{обн.стр.}}$ — время обнаружения КА по структуре [2].

$$P_{\text{св.обн. стат.}}(t) = 1 - e^{\left(-\frac{T_{\text{обн. тр.}}}{t_{\text{обн. стат.}}}\right)}, \tag{6}$$

где $T_{\text{обн.стат.}}$ — время обнаружения КА по статистике.

$$P_{\text{дост.обн. КА}}(t) = P_{\text{дост. обн. стр.}}(t) \times P_{\text{дост. обн. стат.}}(t), \tag{7}$$

где $P_{\text{дост.обн.стр.}}(t)$ — вероятность достоверного обнаружения КА по структуре; $P_{\text{дост.обн.стат.}}(t)$ — вероятность достоверного обнаружения КА по статистике.

$$P_{\text{дост.обн. стр.}}(t) = 1 - P_{\text{ош.обн. стр.}}(t), \tag{8}$$

где $P_{\text{ош.обн.стр.}}(t)$ — вероятность ошибочного обнаружения КА по структуре.

$$P_{\text{ош.обн. стр.}}(t) = 1 - e^{\left(-\frac{T_{\text{обн. тр.}} - t_{\text{обн. стр.}}}{T_{\text{обн. тр.}}}\right)}. \tag{9}$$

$$P_{\text{дост.обн. стат.}}(t) = 1 - P_{\text{ош.обн. стат.}}(t), \tag{10}$$

где $P_{\text{ош.обн.стат.}}(t)$ — вероятность ошибочного обнаружения КА по статистике.

$$P_{\text{ош.обн. стат.}}(t) = 1 - e^{\left(-\frac{T_{\text{обн. тр.}} - t_{\text{обн. стат.}}}{T_{\text{обн. тр.}}}\right)}. \tag{11}$$

В выражениях (5)–(11) рассматривается зависимость $P_{\text{св.обн.стр.}}(t)$, $P_{\text{св.обн.стат.}}(t)$, $P_{\text{ош.обн.стр.}}(t)$, $P_{\text{дост.обн.стат.}}(t)$ от $T_{\text{обн.стр.}}$ и $T_{\text{обн.стат.}}$

Гипотетические графики, отображающие зависимость вероятности своевременного и достоверного обнаружения КА от времени их обнаружения в ЛВС, для существующих и перспективных систем обнаружения вторжений представлены на рис. 1 и 2.

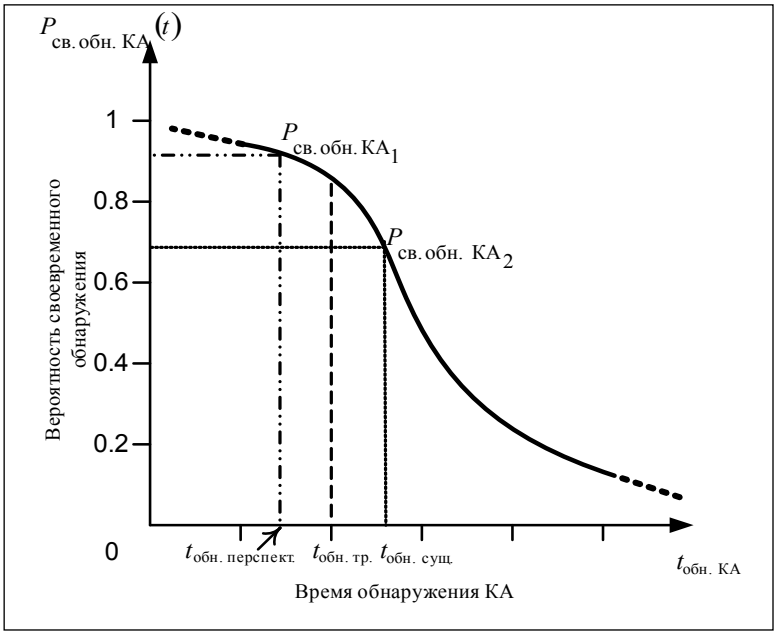

Рис. 1. Гипотетический график зависимости вероятности своевременного обнаружения КА от времени их обнаружения в ЛВС

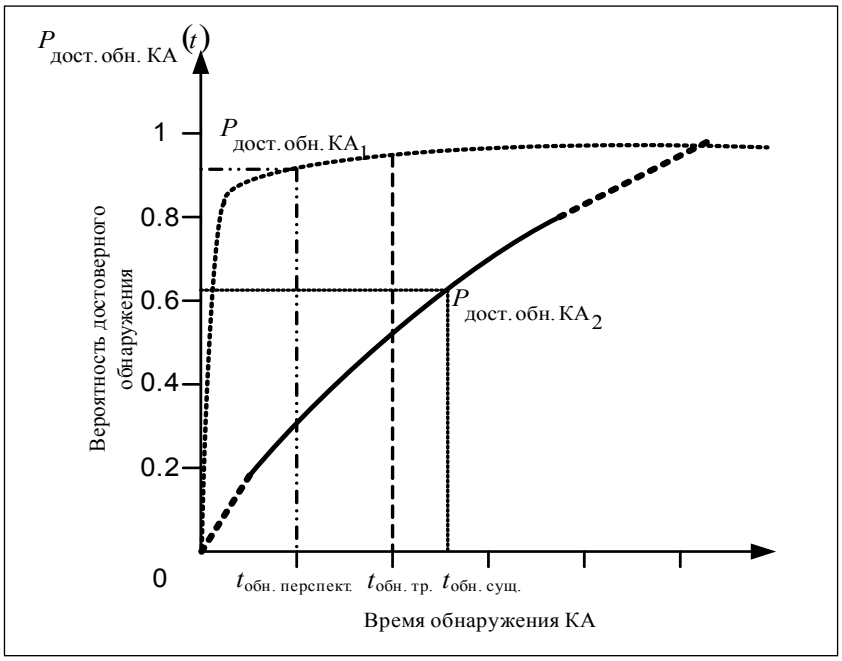

Рис. 2. Гипотетический график зависимости вероятности достоверного обнаружения КА от времени их обнаружения в ЛВС

Представленные на графиках (Рис. 1 и 2) обозначения имеют следующий физический смысл: $P_{\text{св.обн.КА}}(t)$ – вероятность своевременного обнаружения КА; $P_{\text{дост.обн.КА}}(t)$– вероятность достоверного обнаружения КА; $t_{\text{обн.перспект.}}$ – время обнаружения КА перспективное; $t_{\text{обн.сущ.}}$– время обнаружения КА существующее; $t_{\text{обн.тр.}}$ – требуемое время обнаружения КА; $P_{\text{св.обн.КА}_1}$– вероятность своевременного обнаружения КА при $t_{\text{обн.перспект.}}$; $P_{\text{св.обн.КА}_2}$– вероятность своевременного обнаружения КА при $t_{\text{обн.сущ.}}$; $P_{\text{дост.обн.КА}_1}$– вероятность достоверного обнаружения КА при $t_{\text{обн.перспект.}}$; $P_{\text{дост.обн.КА}_2}$– вероятность достоверного обнаружения КА при $t_{\text{обн.сущ.}}$.

Таким образом, введенные показатели позволяют количественно оценить эффективность функционирования как собственно ЛВС, так и их систем обнаружения вторжений в условиях воздействия КА в метрике «своевременность-достоверность».

СПИСОК ЛИТЕРАТУРЫ:

1. *Бусленко Н. П.* Моделирование сложных систем. М.: Наука, 1978.
2. *Вентцель Е. С., Овчаров Л. А.* Теория вероятностей и ее инженерные приложения. М.: Наука, 1988.