В качестве меры согласованности используется индекс согласованности. Согласованность матрицы $[Sp_{m\times m}]$ эквивалентна требованию равенства ее максимального собственного значения $\lambda_{max}$ числу сравниваемых объектов $n$, то есть $\lambda_{max} = n$. В качестве меры несогласованности мнений экспертов рассматривается нормированное отклонение $\lambda_{max}$ от $n$, называемое индексом согласованности (ИС):

$$\text{ИС} = \frac{\lambda_{max} - n}{n - 1}.$$

Получив индекс согласованности и выбрав по таблицам случайный индекс для заданного порядка матрицы, определяется отношение согласованности (ОС)

$$\text{ОС} = \text{ИС} / \text{СИ}.$$

Если величина ОС ≤ 0,1, то степень согласованности экспертных данных считается приемлемой. В противном случае (если ОС > 0,1) эксперту рекомендуется пересмотреть свои суждения. Для этого необходимо выявить те позиции в матрице суждений, которые вносят максимальный вклад в величину отношения согласованности, и попытаться изменить меру несогласованности в меньшую сторону на основе более глубокого анализа вопроса.

### *ВЫВОДЫ*

Разработаны математические модели предметной области проектирования СППР охраняемого объекта и инструментальные средства СППР по ликвидации нештатных ситуаций.

Усовершенствованы многоальтернативные процедуры принятия решений с оцениванием человеческого и технико-экономических факторов в принятии решений по ликвидации нештатных ситуаций.

Разработана математическая модель и вычислительная процедура выбора рационального состава комплекса технических средств СППР.

Разработаны информационное и программное обеспечения процесса поддержки принятия решений оператором по ликвидации нештатных ситуаций.

### *ПЕРЕЧЕНЬ ССЫЛОК*

1. *Саати Т.* Принятие решений. Метод анализа иерархий / Т. Саати. – М. : Радио и связь, 1989. – 316 с.
2. Системи підтримки прийняття рішень : навчальний посібник / О. І. Пушкар, В. М. Гіковатий, О. С. Євсєєв, Л. В. Потрашкова / За ред. д-ра екон. наук, проф. Пушкаря О. І. – Х. : «ІНЖЕК», 2006. – 304 с.
3. *Ерохин А. Л.* Система поддержки принятия решений при авариях в энергосистемах / А. Л. Ерохин // Проблемы бионики. – 1999. – Вып. 50. – С. 157–161.
4. *Гриб О. Г.* Система поддержки принятия решения при аварийных ситуациях в энергосистемах / О. Г. Гриб, О. Н. Довгалюк, А. Л. Ерохин // Світлотехніка та електроенергетика. – 2008. – № 4. – С. 64–68.

Надійшла 11.05.2009

*Розроблено структура, склад і інформаційні технології підтримки ухвалення рішень по ліквідації нештатних і аварійних ситуацій, які контролюються охоронно-пожежною сигналізацією. Приведено приклад вибору комплексу апаратно-програмних засобів за сукупністю локальних критеріїв, якими виступають техніко-економічні показники ефективності ухвалення рішень по ліквідації нештатних ситуацій.*

*There have been developed a structure, body and information technologies for decision-making support in terms of handling off-nominal situations being controlled by fire and security alarm. There is given an example of choosing a complex of physical and programme means basing on the set of criteria, the latter being technical and economic indicators of decision-making efficiency in terms of handling off-nominal situations.*

*УДК 004.056*

А. Е. Архипов

# ЭКСПЕРТНО-АНАЛИТИЧЕСКОЕ ОЦЕНИВАНИЕ ИНФОРМАЦИОННЫХ РИСКОВ И УРОВНЯ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

*Рассматриваются некоторые особенности применения методологии информационных рисков для исследования защищенности информационных систем, в частности, практические подходы к оцениванию количественных показателей, используемых для вычисления информационных рисков, а также показателей защищенности информационных систем и эффективности систем защиты информации.*



### *ВВЕДЕНИЕ*

Действующие международные стандарты [1–3] настойчиво рекомендуют методологию оценивания и управления информационными рисками как действенный инструмент исследования угроз безопасности информационных систем (ИС), оценивания уровня

защищенности этих систем, анализа эффективности функционирования систем защиты информации. К сожалению, высокий потенциал методологии информационных рисков на практике в значительной мере ограничивается необходимостью использования в ней плохо поддающихся определению в условиях практики количественных значений вероятностей реализации тех или иных угроз информации и количественных оценок ущерба (потерь), обусловленных успешной реализацией этих угроз. В максимальной степени это касается угроз несанкционированного доступа (НСД), связанных с наличием плохо прогнозируемого человеческого фактора.

### *ПОСТАНОВКА ЗАДАЧИ*

Риск $R(T)$, определяющий вероятные потери $q(T)$, обусловленные реализацией угрозы $T$, определяется выражением

$$R(T)=P(T)q(T), \qquad (1)$$

где $P(T)$ – вероятность реализации угрозы $T$. Для множества угроз $\{T_i\}$, $i = \overline{1, N}$ количественные значения $P(T_i)$, $q(T_i)$ задаются, как правило, путем их прямого экспертного оценивания, что приводит к высокому уровню субъективной ошибки в получаемых оценках параметров. Поэтому в ряде случаев оправданным оказывается применение качественных оценок вероятности ущерба. При этом в обоих случаях уровень погрешностей в итоговой оценке риска резко снижает эффективность и результативность анализа рисков.

Исправить эту ситуацию можно применением экспертно-аналитического подхода к получению оценок $P(T_i)$, $q(T_i)$, $i = \overline{1, N}$, суть которого во введении определенной детализации и структуризации процедур нахождения экспертных оценок соответствующих параметров рисков.

### *СЦЕНАРНАЯ МЕТОДОЛОГИЯ НАХОЖДЕНИЯ ОЦЕНКИ УЩЕРБА, ОБУСЛОВЛЕННОГО РЕАЛИЗАЦИЕЙ УГРОЗ ИНФОРМАЦИИ*

В [4] для оценивания уровня ущерба $q$ предложено использовать метод сценариев, базирующийся на рассмотрении и интегральном учете последствий ряда возможных сценариев развития событий, обусловленных реализацией угрозы $T_i$. Сценарии образуют множество $\{Sc_l\}$, $l = \overline{1, k}$, каждому элементу которого ставится в соответствие двойка $<P_l, Q_l>$, где $P_l$ – вероятность осуществления $l$-го сценария, а $Q_l$ – характеристика ущерба (потерь), причиняемого ИС либо информационным ресурсам по завершению развития соответствующего сценария.

Проблемным аспектом оценивания интегрального ущерба в схеме сценариев является построение способа свертки частных потерь $Q_l$, $l = \overline{1, k}$, в результирующее значение $q$. Обычная свертка вида $\sum P_l Q_l$ вследствие возможности одновременного параллельного развития ряда сценариев приводит к завышенной оценке интегрального ущерба [4, 5]. Поэтому в общем случае для исходного ансамбля возможных сценариев $\{Sc_1, Sc_2, \ldots, Sc_k\}$ конструируется полная группа возможных исходов $\{Z_1, Z_2, \ldots, Z_m\}$, $m = 2^k$ с указанием их вероятностей $P(Z_j)$, $j = \overline{1, m}$ и частных ущербов $Q(Z_j)$. Так, для ансамбля из трех сценариев $\{Sc_1, Sc_2, Sc_3\}$ с соответствующим набором элементарных исходов $\{V_1, V_2, V_3\}$ получаем полную группу событий $\{Z_1, Z_2, \ldots, Z_8\}$, где $Z_1 = V_1 \cap V_2 \cap V_3$, $Z_2 = V_1 \cap V_2 \cap \overline{V}_3$, $\ldots$, $Z_j = \overline{V}_1 \cap V_2 \cap \overline{V}_3$, $\ldots$, $Z_8 = \overline{V}_1 \cap \overline{V}_2 \cap \overline{V}_3$.

События $Z_1, \ldots, Z_8$, составленные из исходов $V_1$, $V_2$, $V_3$ и противоположных им элементов $\overline{V}_1$, $\overline{V}_2$, $\overline{V}_3$, является попарно несовместимыми, а для их вероятностей справедливы соотношения: $\sum_{j=1}^{\cup} P(Z_j) = 1$, $P(Z_j + Z_g) = P(Z_j) + P(Z_g)$ и $P(Z_j Z_g) = 0$ при $j \neq g$.

В соответствии со структурой событий $Z_j$, $j = \overline{1, 8}$ рассчитываются их вероятности и частные ущербы [4]: $P(Z_1) = P_1 P_2 P_3$, $P(Z_2) = P_1 P_2 (1-P_3)$, $\ldots$, $P(Z_j) = (1-P_1) P_2 (1-P_3)$, $\ldots$, $P(Z_8) = \prod_{j=1}^{\cup} (1-P_j)$, $Q(Z_1) = Q_1 + Q_2 + Q_3$, $Q(Z_2) = Q_1 + Q_2$, $\ldots$, $Q(Zj) = Q_2$, $\ldots$, $Q(Z_8) = 0$.

Для расчета интегрального ущерба $q$ после перехода к полной группе событий применение свертки вполне корректно:

$$q = \sum_{j=1}^{m} P(Z_j) Q(Z_j) = \sum_{j=1}^{m-1} P(Z_j) Q(Z_j). \qquad (2)$$

В принципе возможна более глубокая проработка сценариев, ведущая к их детализации и представлению в виде графа взаимосвязанных промежуточных сцен с иерархической (древовидной) структурой [4], что позволяет говорить об использовании системного подхода в реализации основных положений изложенной методики нахождения интегральной оценки потерь $q$. Конкретизация источников происхождения потерь $Q(Z_j)$ в реальной ситуации позволит опредметить процессы образования потерь (ущербов), более четко проанализировать характер и количественные параметры потерь в конкретных предметно-прикладных аспектах, в частности, получить точные и объективные экспертные оценки $P(Z_j)$ и $Q(Z_j)$.

### *ОЦЕНИВАНИЕ ВЕРОЯТНОСТНЫХ ПАРАМЕТРОВ МОДЕЛИ УГРОЗ*

Для нахождения вероятности $P(T)$ применение прямой экспертной оценки также не дает приемлемых результатов, при этом уровень субъективных ошибок оценивания оказывается зависимым от подбора экспертов. Эксперты, являющиеся сотрудниками организации, информация которой подлежит защите, т. е. «внутренние эксперты», достаточно хорошо осознают уязвимости системы защиты и защищаемых информационных ресурсов, что и находит свое отражение в их субъективных оценках вероятности $P(T)$. Оценки же «внешних» экспертов в большей степени учитывают специфические потребительские свойства защищаемого ресурса, мотивирующего злоумышленника к попыткам овладеть этим информационным ресурсом, уничтожить его либо исказить его содержание. В этом случае перспективным оказывается применение так называемой двухфакторной модели оценки вероятности $P(T)$, позволяющей в общей вероятности реализации угрозы выделить два компонента (фактора), один из которых отображает мотивационную составляющую возникновения угрозы, а второй учитывает существующие уязвимости. В итоге имеем [5]:

$$P(T) = p(T)p(a_T), \qquad (3)$$

где $p(T)$ – вероятность возникновения (актуализации) угрозы $T$, $p(a_T)$ – вероятность наличия совокупности уязвимостей, позволяющих реализовать угрозу $T$. По своей сути $p(a_T)$ – обобщенная вероятность успешного проведения комплекса атак, обусловленных (порождаемых) упомянутой совокупностью уязвимостей защищаемой ИС (включая уязвимости самой системы защиты информации (СЗИ)).

В частности, для оценивания вероятности возникновения угрозы можно использовать предложенное в [6] соотношение, позволяющее в первом приближении полагать

$$p(T) \approx 1 - \frac{D}{d}, \qquad (4)$$

где $D$ – общая стоимость затрат атакующей стороны на реализацию угрозы $T$, $d$ – полученный при этом «выигрыш», определяемый ценностью защищаемого ресурса $I$ для злоумышленников.

Ясно, что если ценность ресурса $I$ для атакующей стороны очень высока, злоумышленники готовы идти на значительные затраты средств для реализации угрозы $T$. Поэтому в случае $d >> D$ вероятность $p(T)$ будет практически равна 1. При малых значениях $d$ мотивированность злоумышленников к реализации угрозы $T$ низка, в частности при $d = D$ теоретически $p(T) = 0$, а при $d < D$ формула (4) теряет смысл. На практике это означает, что вероятность применения для реализации угроз высокозатратных атак низка. Атаки, подготовка, организация и проведение которых сопряжены со значительными затратами, оправданы лишь в случае, если, например, информация $I$ составляет государственную тайну, т. е. уровень ее значимости может быть чрезвычайно высок, поэтому даже для значительных $D$ отношение $D/d < 1$. Кроме того, важным аспектом в анализе вероятности затратных атак является то, что их организация и проведение связаны со значительными финансовыми рисками, позволить которые себе могут далеко не многие фирмы или организации.

При грубом упрощенном оценивании вероятность $p(T)$ может задаваться равной 0 или 1. В последнем случае вероятность реализации угрозы $p(T)$ фактически оказывается тождественной вероятности успешного проведения комплекса атак $p(a_T)$.

При оценке вероятности $p(a_T)$, учитывая, что ее значение непосредственно связано с наличием и характером возможных уязвимостей ИС и СЗИ, приходим к необходимости детализации обстоятельств, связанных с возможностью реализации угроз, приводящей к некоторой иерархической многоуровневой структуре «источник угроз – уязвимости – атаки – угрозы – потери». При анализе реальной ИС этой структуре будет соответствовать направленный граф, позволяющий зафиксировать связи элементов, составляющих все перечисленные уровни, что, в частности, разрешит построить расчетные соотношения для вычисления вероятности $P(T)$. Для этого, выделив совокупность атак $\{a_{si}\}$, $s = \overline{1, K_i}$, где $K_i$ – объем множества атак, направленных на реализацию угрозы $T_i$, получаем выражение для расчета вероятности $p(a_{Ti})$ через вероятности осуществления атак $p(a_{si})$ [5]:

$$p(a_{Ti}) = 1 - \prod_{s=1}^{K_i} [1 - p(a_{si})]. \qquad (5)$$

Вероятности атак $p(a_{si})$ $s = \overline{1, K_i}$, так же как и вероятности возникновения угроз $p(T_i)$, $i = \overline{1, N}$, задаются путем прямого экспертного оценивания, обеспечивая учет особенностей и свойств реальной ИС. Аналогичным путем оцениваются вероятности осуществления остальных угроз.

Завершающим этапом анализа рисков является вычисление интегрального информационного риска $R_t$, обобщающего значения частных рисков, обусловленных реализациями тех или иных угроз в ИС. При расчете $R_t$ возникают сложности, аналогичные уже рассмотренной выше проблеме свертки частных потерь $Q_l$ , $l = \overline{1, k}$ в оценку интегрального ущерба $q$. В частности, группа угроз $\{T_i\}$, $i = \overline{1, N}$ не образует полной группы событий, достаточной для описания и количественной оценки уровня защищенности ИС [5].

Поэтому традиционно рассматриваемую тройку угроз конфиденциальности, доступности и целостности информации (соответственно $T_1$, $T_2$, $T_3$), к реализации которых обычно стремятся свести имеющееся множество атак, следует преобразовать в полную группу из восьми комплексных угроз, содержащих все возможные сочетания исходных угроз: $\{T_1T_2T_3\}$, $\{T_1T_2\}$, $\{T_1T_3\}$, $\{T_2T_3\}$, $\{T_1, T_2, T_3\}$. Для формирования полной группы вводятся события, противоположные угрозам: $\overline{T}_1$, $\overline{T}_2$, $\overline{T}_3$, которые формально можно трактовать как события, соответствующие отсутствию факта актуализации(возникновения) соответствующей прямой угрозы конфиденциальности, доступности, целостности. Учитывая возможность существования комплексного события, состоящего в невозможности реализации какой-либо угрозы, получаем полную группу событий, соответствующих восьми комплексным угрозам: $T_{r_1} = T_1 \cap T_2 \cap T_3$, $T_{r_2} = T_1 \cap T_2 \cap \overline{T}_3$, …, $T_{r_l} = \overline{T}_1 \cap T_2 \cap \overline{T}_3$, $T_{r_8} = \overline{T}_1 \cap \overline{T}_2 \cap \overline{T}_3$. Для каждого компонента этой полной группы, как это уже выполнялось выше для событий $\{Z_1, \ldots, Z_8\}$, можно рассчитать соответствующие вероятности и комплексные ущербы, представимые множеством двоек $\{P(Tr_l), Q(Tr_l)\}$, $l = \overline{1,8}$, после чего найти информационный риск ИС в целом. Например, $P(Tr_1) = P(T_1) \times \times P(T_2)P(T_3)$, $P(Tr_2) = P(T_1)P(T_2)[1-P(T_3)]$, …, $P(Tr_l) = [1-P(T_1)]P(T_2)[1-P(T_3)]$, …, $P(Tr_8) = [1-P(T_1)][1-P(T_2)][1-P(T_3)]$. Далее, принимая гипотезу аддитивности ущерба, обусловленного реализацией комплексной атаки [5], получаем: $q(Tr_1) = q_1 + q_2 + q_3$, $q(Tr_2) = q_1 + q_2$, …, $q(Tr_l) = q_2$, …, $q(Tr_8) = 0$, где $q_1$, $q_2$, $q_3$ – ущербы, обусловленные реализациями соответствующих угроз $T_1, T_2, T_3$.

Окончательная формула для расчета информационного риска, обусловленного угрозами $T_1, T_2, T_3$ имеет вид:

$$R_T = \sum_{j=1}^{'} P(Tr_j)q(Tr_j). \qquad (6)$$

## ОЦЕНИВАНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Осуществление в ИС каких-либо защитных мероприятий ведет к уменьшению вероятностей $p(a_{si})$ успешного проведения комплекса атак, а, следовательно, к обновлению (уменьшению) значений $P(Tr_j)$ в формуле (6) и к новому расчетному значению риска $R_{TO}$, называемого в этом случае остаточным. Результативность проведенных защитных мероприятий определяется в первую очередь значением «снятого» риска $\Delta R = R_T - R_{TO}$, его приведенными значениями $\Delta R/R_{TO}$ либо $\Delta R/R_T = 1-(R_{T0}/R_T)$. Последнее является показателем защищенности ИС, характеризующимся удобной измерительной шкалой с диапазоном возможных значений от 1 (случай «абсолютной защищенности, $T_{T0} = 0$) до 0 (нулевая эффективность СЗИ, $R_T = R_{T0}$, $\Delta R = 0$).

Расширенный показатель эффективности системы защиты информации, учитывающий затраты $C$ на создание и обслуживание системы защиты, имеет вид [7]:

$$w = (\Delta R - C)/C. \qquad (7)$$

В соответствие с формулой (7) наиболее эффективной СЗИ будет та, которая обеспечивает максимум предотвращенного ущерба на единицу затрат, обусловленных построением СЗИ и ее обслуживанием в течение определенного промежутка времени.

## ВЫВОДЫ

Результативность применения методологии информационных рисков в исследовании защищенности информационных систем во многом определяется точностью используемых для вычисления информационных рисков количественных параметров, определяющих вероятности угроз и уровни возникающих при их реализации потерь. Оценивание этих параметров на практике сталкивается с серьезными трудностями, вынуждающими применять прямые экспертные методы задания искомых параметров, что нередко приводит к существенному снижению точности результатов исследований. Избежать этих негативных последствий можно, применив изложенные выше экспертно-аналитические методы оценивания количественных параметров, используемых при расчете рисков.

## ПЕРЕЧЕНЬ ССЫЛОК


1. ISO/IEC 2700:2005. Information Technology – Security techniques – Information security management systems – Requirements [Електронний ресурс] : Secretariat ISO/IEC JTC 1/SC 27, DIN Deutsches Institut für Normung Berlin, Germany. – Режим доступу : http://www.jtc1sc27.din.de/en. – Назва з екрана.
2. ISO/IEC 27002:2007, Information Technology – Security techniques – Code of practice for information security management [Електронний ресурс] : Secretariat ISO/IEC JTC 1/SC 27, DIN Deutsches Institut für Normung Berlin, Germany. – Режим доступу : http://www.jtc1sc27.din.de/en. – Назва з екрана.
3. ISO/IEC 27005, Information Technology – Security techniques – Information security risk management [Електронний ресурс]: Secretariat ISO/IEC JTC 1/SC 27, DIN Deutsches Institut für Normung Berlin, Germany. – Режим доступу : http://www.jtc1sc27.din.de/en. – Назва з екрана.
4. *Архипов О. Є.* Застосування методології передбачення для оцінювання шкоди, заподіяної витоком секретної інформації / О. Є. Архипов, І. П. Касперський // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип. 2 (15). – К. : 2007. – С. 13–19.
5. *Архипов А. Е.* Применение среднего риска для оценивания эффективности защиты информационных систем / А. Е. Архипов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип. 1 (14). – К. : 2007. – С. 60–67.

6. *Архипов А. Е.* Применение мотивационно-стоимостных моделей для описания вероятностных соотношений в системе «анализ – защита» / А. Е. Архипов, С. А. Архипова // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип. 1 (16). – К. : 2008. – С. 57–61.
7. *Архипов О. Є.* Оцінювання ефективності системи охорони державної таємниці / О. Є. Архипов, І. Т. Бородавко, В. П. Ворожко. – К. : Наук.-вид. від-діл НА СБ України, 207. – 63 с.

Надійшла 16.02.2009
Після доробки 17.03.2009

*Розглянуто деякі особливості застосування методології інформаційних ризиків до дослідження захищеності інформаційних систем, зокрема практичні підходи до оцінювання кількісних показників, що використовуються для обчислення інформаційних ризиків, а також показників захищеності інформаційних систем та ефективності систем захисту інформації.*

*In this paper some features of information risk methodology application for information systems security research, in particular practical estimation approaches of the quantity indicators used for calculation information risk, and also parameters of information systems security and efficiency of information protection systems are considred.*

*УДК 004.43*

В. М. Крищук, О. Ю. Малий, О. Ю. Воропай

# УНІВЕРСАЛЬНА АЛГОРИТМІЧНА МОВА ПРОГРАМУВАННЯ МІКРОКОНТРОЛЕРІВ

*Досліджено існуючі методи створення алгоритмічних мов програмування. Розроблено універсальну мову програмування мікроконтролерів, що дозволяє переводити програми з одного мікроконтролера в інший, а також задавати загальний алгоритм програми при роботі з любим видом мікроконтролерів.*

## *ВСТУП*

Достатня кількість різних сімейств мікроконтролерів, а також відмінності між мікроконтролерами усередині одного сімейства вимагає розробки методів створення універсального засобу, що могло б дозволити робити налагодження пристроїв на основі мікроконтролерів будь-якого типу. Першим етапом на шляху створення такого засобу є розробка універсальної алгоритмічної мови програмування мікроконтролерів, що дозволить врахувати всі особливості кожного з обраних для роботи мікроконтролерів.

Для створення такої мови необхідно вивчити формальну граматику мов програмування, а також визначити метод універсального опису мікроконтролерів, що дозволив би не тільки описувати існуючі на сьогоднішній день мікроконтролери з усіма виконуваними ними функціями, але і давав можливість розширення достатку виконуваних мікроконтролерами функцій, для опису подальших апаратних розробок структур мікроконтролерів. Для цього пропонується врахувати особливості виконання однієї і тієї ж задачі на різних типах мікроконтролерів, включаючи й апаратну реалізацію задачі, що дозволить провести аналіз і знайти загальні риси роботи. Для чого необхідно проаналізувати особливості перетворення програми, написаної для одного типу мікроконтролера, в програму для іншого типу чи підтипу усередині одного сімейства [1].

## *АНАЛІЗ КОНСТРУКЦІЙ МОВ ПРОГРАМУВАННЯ*

Реакція комп'ютера на данні, що вводяться, однозначна – першою справою занести їх до пам'яті, забезпечивши повну схоронність і чекати подальших команд.

Формально мова програмування – це відкрита безліч текстів, написаних за допомогою деякого набору символів – алфавіту мови. За основним своїм призначенням мова програмування – це засіб спілкування між користувачем і комп'ютерною системою.

Синтаксис мов програмування – сукупність вимог, яким повинна задовольняти будь-яка осмислена програма.

Для завдання синтаксичних правил найбільшою популярністю користується апарат форм Бакуса – Наура. Їхнє основне призначення визначити, які саме послідовності символів вважаються програмами в даній мові програмування. Це досягається вказівкою з яких складових частин і яким способом можуть бути побудовані програми [2].

Семантика мови програмування – це правила, що визначають, які операції і у якій послідовності повинна виконати машина, що працює по довільній заданій їй програмі.

Семантика мови програмування в цілому задається вказівкою:

1. Використовуваних у мові типів (тобто множин) простих значень, наприклад цілих і нецілих чисел.