нормативне та метрологічне забезпечення систем захисту інформації в Україні", НТУ України "КПІ" Міносвіти і науки України, ДСТСЗІ СБ України, випуск № 7, 2003. С. 62 – 77. ***4****. Шорошев В. В., Проскурін В. М., Маєвський Є. Л. Три узагальнених критерії замість сукупності часткових щодо експертної оцінки захищеності інформації від несанкціонованого доступу в автоматизованих (комп'ютерних) системах. Журнал Держкомзв'язку та інформатизації України "Зв'язок" № 5, 2003р. С. 50 – 56.* ***5****. Лукацкий А. В. Обнаружение атак. – 2-е изд., СПб.: БХВ-Петербург, 2003. – 608с.:ил.*

УДК 65.012.8.

МЕТОД ПРОЕКТИРОВАНИЯ ОПТИМАЛЬНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Виталий Носов, Александр Манжай
Национальный университет внутренних дел, г. Харьков

Анотація: **Пропонується модель побудови системи захисту інформації, метод оцінки її ефективності та можливі критерії оптимізації.**
Summary: **The construction model of the defence information system, its efficiency estimation method and possible criteria of optimization, are offered.**
Ключевые слова: **Информационная безопасность, система защиты информации, модель системы защиты информации, оценка рисков, критерии оптимизации системы защиты информации.**

I Введение

Актуальность информационной безопасности в современном, стремительно развивающемся информационном сообществе не вызывает сомнений. За последнее время было опубликовано и издано большое количество трудов, посвященных различным аспектам защиты информации, и все они решали вполне конкретные задачи в этой многогранной проблеме. Как и в большинстве прикладных областей научных знаний, в теории и практике защиты информации постоянно идёт процесс развития и корректировки основных положений, что связано, прежде всего, с развитием самих информационных технологий.

Закрепление тех или иных результатов исследований в области информационной безопасности происходит в виде национальных или международных стандартов и других нормативных документов. На сегодняшний день существует достаточное количество как отечественных, так и зарубежных стандартов и нормативных документов, регламентирующих отдельные аспекты информационной безопасности. Тем не менее, пока в этих документах не определены общепризнанные подходы по оптимизации по различным критериям создаваемой системы защиты информации (СЗИ). Определение этих подходов, их апробация и нормативное закрепление позволит на практике системно и комплексно проектировать СЗИ с последующей обоснованной оценкой её эффективности.

В качестве одного из возможных вариантов предлагается метод проектирования оптимальной СЗИ, учитывающий структуру взаимосвязей объектов защиты внутри информационной системы (ИС), источников угроз, угроз, уязвимостей ИС и механизмов защиты.

II Постановка задачи

Общую зависимость указанных выше основных понятий информационной безопасности (владельцы информации, нарушители, угрозы, уязвимости, риски, контрмеры, информационные ресурсы) весьма наглядно представляет международный стандарт ISO/IEC 15408 "Общие критерии оценки безопасности информационных технологий" (рис. 1).

Анализ отечественной нормативной базы в области информационной безопасности позволил выделить семь этапов в создании СЗИ.

1. Определение информационных ресурсов (ИР), подлежащих защите.
2. Выявление полного множества угроз безопасности ИР, подлежащих защите.
3. Проведение оценки уязвимости и рисков для ИР, подлежащих защите, при выявленном множестве угроз.
4. Разработка проекта (плана) системы защиты информации, снижающего по выбранному критерию риски для ИР, подлежащих защите, при выявленном множестве угроз.
5. Реализация проекта (плана) защиты информации.
6. Определение качества реализованной системы защиты.

7. Осуществление контроля функционирования и управление системой защиты.

Непосредственно проектирование осуществляется на четвёртом этапе, исходными данными для которого должны являться:

- модели:
  - объектов защиты;
  - источников угроз;
  - угроз;
  - уязвимостей ИС;
- оценки рисков для ИР, подлежащих защите.

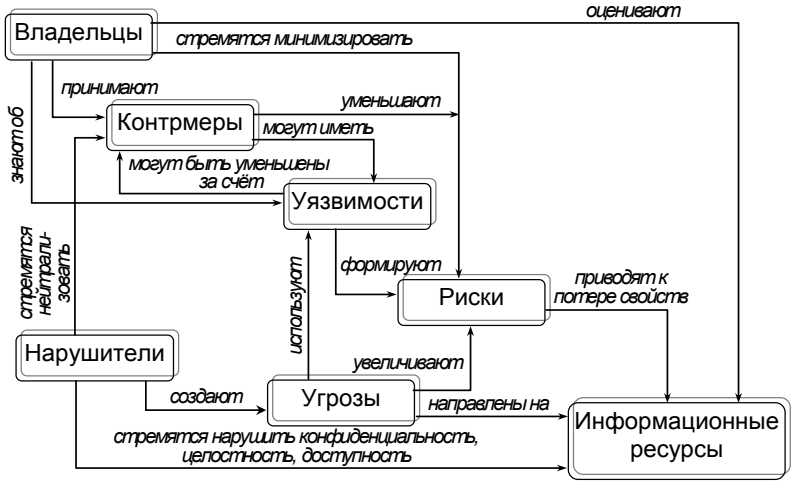

Рисунок 1 – Взаимосвязь основных понятий информационной безопасности

Далее рассмотрим возможные варианты формального описания указанных моделей, схему их взаимодействия, порядок оценки рисков и собственно порядок разработки проекта (плана) СЗИ, снижающего по выбранному критерию риски для ИР, подлежащих защите, при выявленном множестве угроз.

III Модель системы объектов защиты

Целесообразно систему защиты объектов рассматривать не как совокупность отдельных элементов некоторого множества, а как взаимосвязанную структуру элементов, которую можно описать (взяв за основу модель из [1]) в виде четырёхдольного графа (рис. 2).

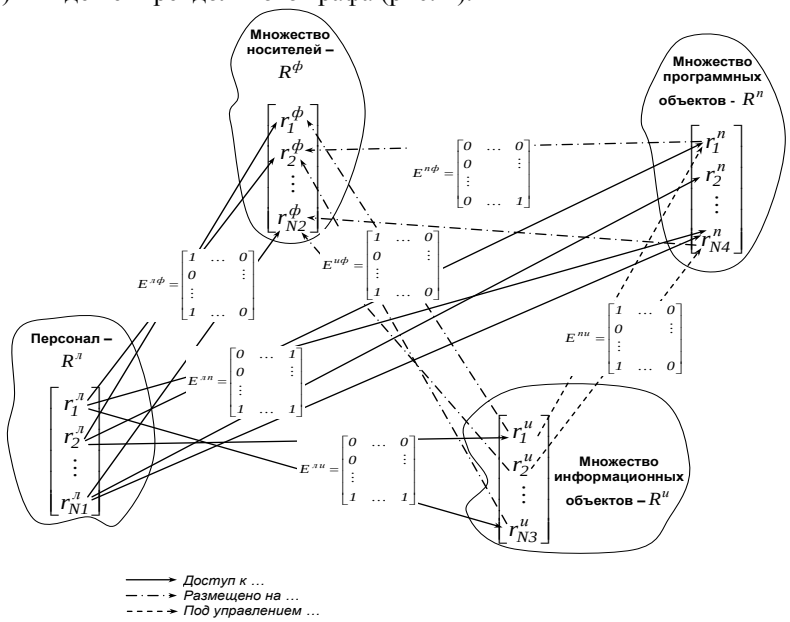

Рисунок 2 - Модель системы объектов защиты

В матричном представлении вершины графа системы объектов защиты представляются четырьмя векторами $R^{л}$, $R^{ф}$, $R^{и}$ и $R^{п}$, элементы которых выражают веса (относительную ценность, стоимость) объектов соответствующих групп. Межгрупповые взаимосвязи, отображаемые дугами графа, выражаются следующими матрицами:

$E^{лф}$ - бинарная прямоугольная матрица размерности $N_1 \times N_2$ (N_1 – количество пользователей, N_2 - количество носителей объектов защиты), описывающая пространство доступа персонала к носителям (1 – разрешен доступ, 0 – нет доступа);

$E^{ли}$ - бинарная прямоугольная матрица размерности $N_1 \times N_3$ (N_3 – количество информационных объектов), описывающая пространство доступа персонала к информационным ресурсам системы (1 – есть доступ, 0 – нет доступа);

$E^{лп}$ - бинарная прямоугольная матрица размерности $N_1 \times N_4$ (N_4 – количество программных объектов), описывающая пространство доступа персонала к объектам программного обеспечения системы (1 – есть доступ, 0 – нет доступа);

$E^{иф}$ - бинарная прямоугольная матрица размерности $N_2 \times N_3$, описывающая пространство размещения информационных ресурсов на носителях (1 – размещено, 0 – не размещено);

$E^{пф}$ - бинарная прямоугольная матрица размерности $N_2 \times N_4$, описывающая пространство размещения программного обеспечения на носителях (1 – размещено, 0 – не размещено);

$E^{пи}$ - бинарная прямоугольная матрица размерности $N_3 \times N_4$, описывающая пространство управления программным обеспечением информационными объектами системы (1 – управляет, 0 – не управляет).

Весовые коэффициенты $r^{(и,п,ф,л)}$ определяются следующим образом:

$$r^{(и,п,ф,л)} = r_{исх}^{(и,п,ф,л)} \cdot r_{сис}^{(и,п,ф,л)} \tag{1}$$

где – $r_{исх}^{(и,п,ф,л)}$ - вес объекта, определяемый как относительная финансовая стоимость объекта к общим финансовым затратам на приобретение объектов того же рода; $r_{сис}^{(и,п,ф,л)}$ - вес объекта в конкретной ИС с учётом взаимосвязей всех элементов.

Системные веса $r_{сис}^{(и,п,ф,л)}$ можно определить, используя следующие утверждения [1]:

- чем больше и с большим весом пользователей имеют доступ к информационному объекту, тем выше его ценность и значимость в ИС;
- чем больше и более ценных информационных ресурсов находится под управлением данного объекта программного обеспечения (ПО), тем более ценно и важно данное программное обеспечение;
- чем больше и более ценных информационных и программных объектов размещено на данном физическом объекте, тем выше его ценность в ИС;
- чем к большему числу наиболее ценных информационных, программных и физических объектов имеет доступ пользователь, тем выше его вес (значимость в ИС).

Данные утверждения реализуются следующими соотношениями [1]:

$$R_{сис}^{л} = \frac{1}{3}\left(\frac{1}{N_2} E^{лф} \cdot R_{сис}^{ф} + \frac{1}{N_3} E^{ли} \cdot R_{сис}^{и} + \frac{1}{N_4} E^{лп} \cdot R_{сис}^{п} \right) \tag{2}$$

$$R_{сис}^{ф} = \frac{1}{2}\left(\frac{1}{N_3} E^{иф} \cdot R_{сис}^{и} + \frac{1}{N_4} E^{пф} \cdot R_{сис}^{п} \right) \tag{3}$$

$$(R_{сис}^{п})^{T} = \frac{1}{N_3}\left(R_{сис}^{и}\right)^{T} E^{пи} \tag{4}$$

Соотношения (2 – 5) определяют рекурсивную процедуру взаимного учёта весовых коэффициентов при их вычислении по различным группам объектов защиты ИС. На первом шаге значения $r_{сис}$ предполагаются равными единице, после вычисления сходящейся итеративной процедуры получаются

итоговые системные веса объектов защиты.

$$(R^{и}_{сис})^{T} = \frac{1}{N_1}\left(R^{л}_{сис}\right)^{T} E^{лш} \tag{5}$$

Координаты вектора $R^{ф}$ являются относительными весовыми коэффициентами, выражающими значимость информационных объектов для функционирования ИС организации. Абсолютные показатели размещённых на носителях информационных объектов (их стоимость, вектор-столбец $R(r_1,r_2,\ldots,r_{N_2})$) определяются следующим образом:

$$r_i = Y\frac{r_i^{ф}}{\sum_{j=1}^{N_2} r_j^{ф}},\ i=\overline{1,N_2},\ j=\overline{1,N_2} \tag{6}$$

где Y – стоимость всей информации организации, определяемая методом экспертных оценок.

В итоге, выражение (6) позволяет сформировать вектор-столбец $R(r_1,r_2,\ldots,r_{N_2})$ стоимости объектов защиты с учётом их весов в конкретной ИС.

IV Модель воздействия угроз на множество объектов защиты с учётом СЗИ

Модель воздействия угроз на множество объектов защиты с учётом системы защиты информации может быть представлена посредством пятидольного вершинно и реберно взвешенного графа, изображенного на рис. 3.

Вершины графа образуют пять векторов-столбцов S, A, V, C и R, где:

$R(r_1,r_{2,\ldots},r_{N2})$ - вектор-столбец весовых коэффициентов объектов защиты, которые выражают величины стоимости (ущерба) для каждого объекта защиты (см. (6));

$A(a_1,a_2,\ldots,a_M)$ - единичный вектор-столбец M идентифицированных угроз для всех объектов защиты (a_i=1); каждая угроза обозначается соответствующим a_i;

$S(s_1,s_2,\ldots,s_L)$ - вектор-столбец весовых коэффициентов источников угроз, которые выражают степень опасности каждого выявленного источника угроз; значения весовых коэффициентов лежат в диапазоне от 0 (нет опасности) до 1 (степень опасности максимальна); метод формирования этих коэффициентов может быть взят из [2];

$V(v_1,v_2,\ldots,v_L)$ - вектор-столбец весовых коэффициентов уязвимостей объектов защиты, которые выражают степень опасности каждой выявленной уязвимости объекта защиты; значения весовых коэффициентов лежат в диапазоне от 0 (не опасна) до 1 (степень опасности максимальна); метод формирования этих коэффициентов описан в [2];

$C(c_1,c_2,\ldots,c_K)$ - вектор-столбец весов системы защиты информации, в котором коэффициенты $c_1,c_2,\ldots,c_K$ определяют затраты ресурсов (стоимость) на соответствующие элементы СЗИ.

Множество дуг графа, изображенного на рис. 3, можно представить в виде следующих матриц смежности:

SA – бинарная прямоугольная матрица размерности $L\times M$ (L – количество источников угроз, M – количество угроз), описывающая пространство возникновения угроз из их источников, причем каждый элемент матрицы sa_{lm} принимает значение 0 или 1 в зависимости от факта генерации l-ым источником m-ой угрозы;

AV – бинарная прямоугольная матрица размерности $M\times P$ (M – количество угроз, P – количество выявленных уязвимостей объектов защиты), описывающая пространство реализации угроз через уязвимости объектов защиты, причем каждый элемент матрицы av_{mp} принимает значение 0 или 1 в зависимости от факта реализации m-ой угрозы через p-ую уязвимость объектов защиты;

VR – бинарная прямоугольная матрица размерности $P\times N$ (P – количество выявленных уязвимостей объектов защиты, N – количество объектов защиты), описывающая пространство соответствия уязвимостей

объектам защиты, причем каждый элемент матрицы vr_{pn} принимает значение 0 или 1 в зависимости от факта наличия p -ой уязвимости у n -ого объекта защиты;

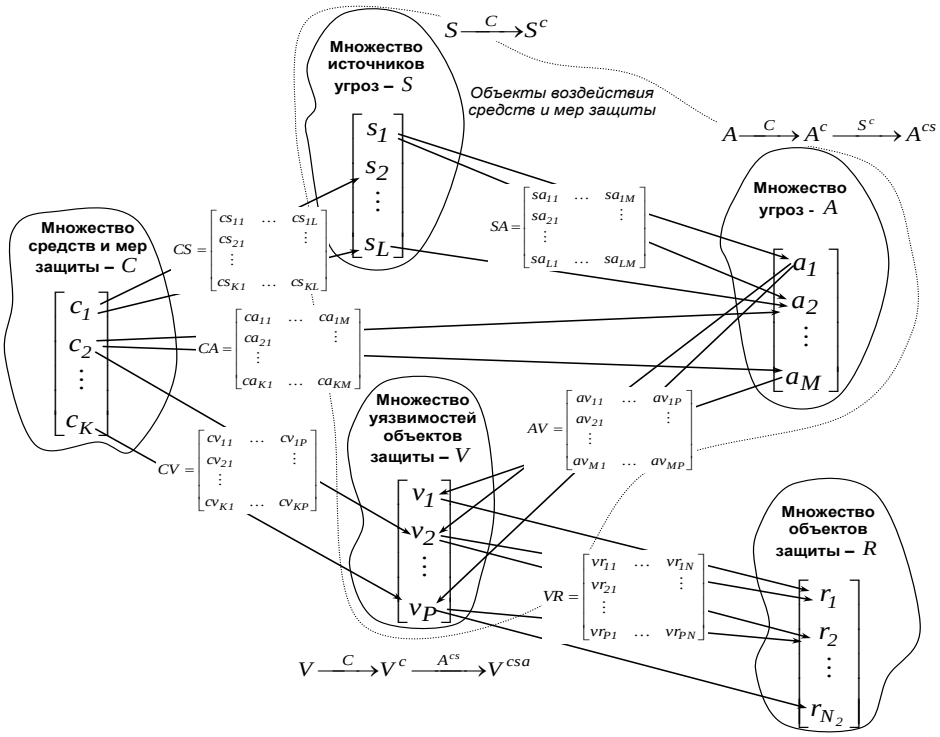

Рисунок 3 - Модель воздействия угроз на множество объектов защиты с учётом системы защиты информации

CS – прямоугольная матрица размерности $K \times L$ (K - количество элементов СЗИ, L - количество источников угроз), описывающая пространство снижения степени опасности источников угроз за счет использования СЗИ, причем элементы матрицы cs_{kl} выражают вероятность нейтрализации k -ым элементом СЗИ l -ого источника угроз;

CA – прямоугольная матрица размерности $K \times M$ (K – количество элементов СЗИ, M – количество угроз), описывающая пространство снижения воздействия угроз на объекты защиты за счет использования СЗИ, причем элементы матрицы ca_{km} выражают вероятность нейтрализации k -ым элементом СЗИ m -ой угрозы;

CV – прямоугольная матрица размерности $K \times P$ (K – количество элементов СЗИ, P – количество выявленных уязвимостей объектов защиты), описывающая пространство снижения степени опасности уязвимостей объектов защиты за счет использования СЗИ, причем элементы матрицы cv_{kp} выражают вероятность нейтрализации k -ым элементом СЗИ p -ой уязвимости.

Воздействие множества средств и мер защиты C на множество выявленных источников угроз S, угроз A и уязвимостей объектов защиты V изменяет степень их опасности ($S \xrightarrow{C} S^c$, $A \xrightarrow{C} A^c$, $V \xrightarrow{C} V^c$), тогда весовые коэффициенты векторов S^c, A^c и V^c определяются выражениями:

$$s_l^c = s_l \left(1 - \prod_{k=1}^{K} (1 - cs_{kl}) \right), \tag{7}$$

$$a_m^c = a_m \left(1 - \prod_{k=1}^{K} (1 - ca_{km}) \right), \tag{8}$$

$$v_p^c = v_p\left(1 - \prod_{k=1}^{K}(1 - cv_{kp})\right). \quad (9)$$

Активизация из S^c хотя бы одного источника m-ой угрозы с учетом СЗИ изменяет вектор угроз A^c ($A^c \xrightarrow{S^c} A^{cs}$), тогда весовые коэффициенты A^{cs} определяются выражением

$$a_m^{cs} = a_m^c\left(1 - \prod_{l=1}^{L} sa_{lm}(1 - s_l^c)\right). \quad (10)$$

Воздействие из A^{cs} хотя бы одной угрозы на p-ую уязвимость объектов защиты с учетом СЗИ изменяет вектор уязвимостей V^c ($V^c \xrightarrow{A^{cs}} V^{csa}$), тогда весовые коэффициенты V^{csa} определяются выражением

$$v_p^{csa} = v_p^c\left(1 - \prod_{m=1}^{M} av_{mp}(1 - a_m^{cs})\right). \quad (11)$$

Пространство СЗИ (вектор-столбец $C(c_1, c_2, \ldots, c_K)$) можно сгруппировать и описать родовидовым деревом. Структуру дерева целесообразно представить в виде двух основных ветвей:

- *обеспечивающие* меры и средства;
  - законодательная, нормативно-правовая, научная и методическая база обеспечения защиты информации;
  - структура и задачи органов (подразделений), обеспечивающих безопасность информационных технологий;
- *основные* меры и средства:
  - организационно-технические и режимные меры и методы защиты информации;
  - программно-технические способы и средства, используемые для защиты информации.

Далее происходит деление основных ветвей по видам мер и средств обеспечения и выполнения функций защиты информации (рис. 4).

Движение от ветвей к листьям "дерева СЗИ" происходит с увеличением детализации мер и средств защиты. В итоге, элементами вектора-столбца $C(c_1, c_2, \ldots, c_K)$ будут затраты ресурсов (стоимость) на реализацию листьев "дерева СЗИ" (рис. 4).

Оценка величин элементов матриц CS, CA и CV представляется возможным только методом экспертных оценок, который может опираться на существующую статистику эксплуатации (если она есть) известных средств защиты. При упрощённом построении (проектировании) СЗИ элементы матриц CS, CA и CV принимаются равными 1, а уже при оценке и испытаниях реализованной СЗИ уточняются.

Представленная модель позволяет далее перейти к оценке риска для ИР.

V Оценка риска для информационных ресурсов

В качестве целевой функции, характеризующей риск для информационных ресурсов, целесообразно использовать величину *относительного потенциального ущерба* E от воздействия совокупности выявленных источников угроз, угроз и уязвимостей объектов защиты с учётом затрат, связанных с использованием СЗИ:

$$E = \frac{C + H}{Y}, \quad (12)$$

где $Y = \sum_{i=1}^{N_2} r_i$ – стоимость всей информации организации;

$C = \sum_{k=1}^{K} c_k$ – стоимость СЗИ;

H – потенциальный ущерб от нарушения информационной безопасности при наличии СЗИ:

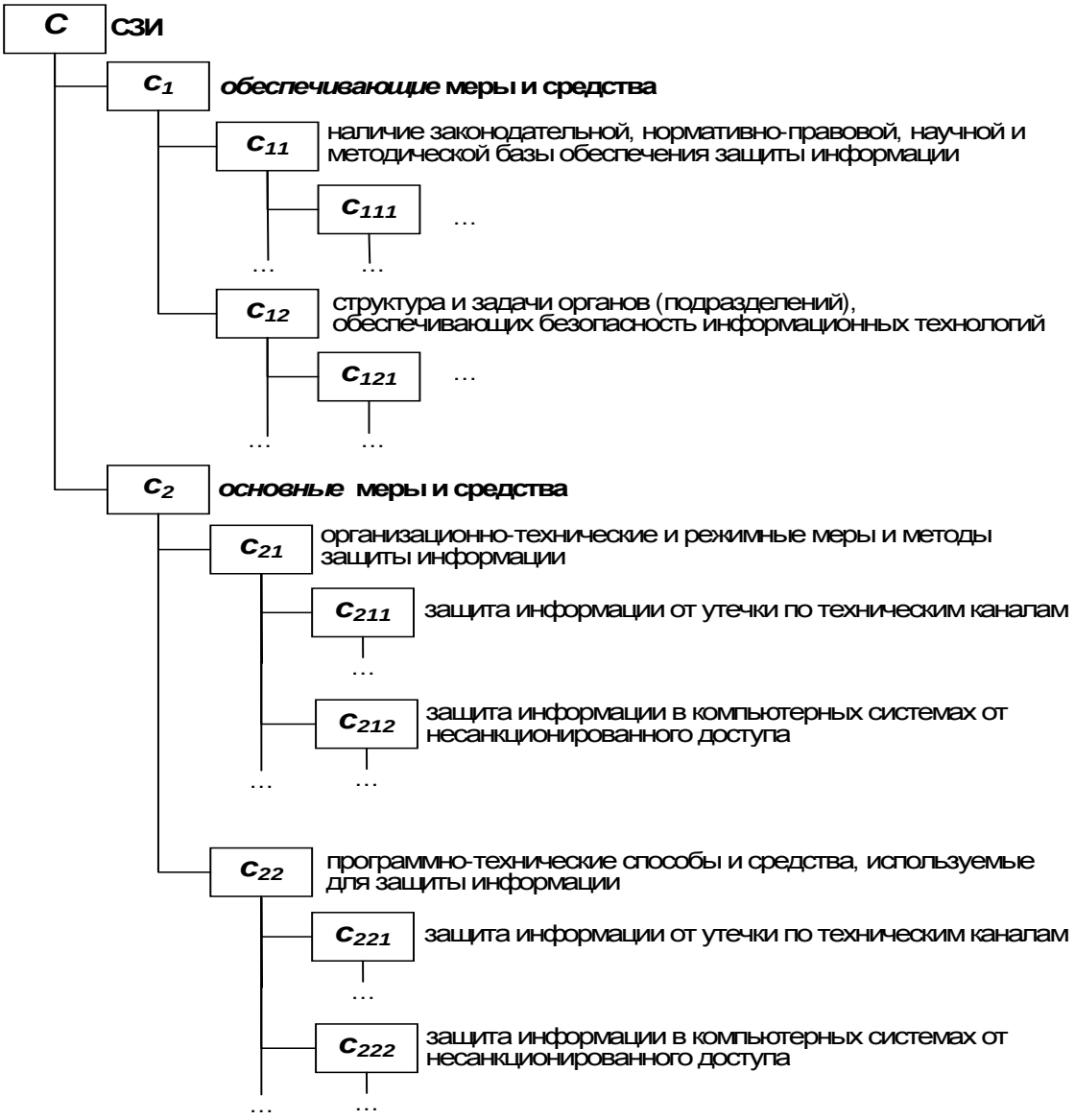

Рисунок 4 - Родовидовое дерево пространства СЗИ

$$H = \sum_{i=1}^{N_2} r_i \left(1 - \prod_{p=1}^{P} vr_{pi}(1 - v_p^{csa}) \right). \qquad (13)$$

При $E = 0$ отсутствует СЗИ и нет потенциальных угроз и ущерба. При $0 < E < 1$ сумма потенциального ущерба и стоимости СЗИ ниже общей стоимости информационных объектов и СЗИ. При $E = 1$ сумма потенциального ущерба и стоимости СЗИ равна стоимости объектов защиты. При $E > 1$ сумма потенциального ущерба и стоимости СЗИ превышает стоимость объектов защиты за счёт стоимости СЗИ.

Величина E является интегральной оценкой риска для всей ИС. Модель воздействия угроз на множество объектов защиты и существующей системы защиты информации (рис. 3) позволяет оценить вклад всех

компонент в интегральную величину E, что позволяет осуществлять управление риском путём решения оптимизационной задачи по выбранным критериям.

VI Критерий и особенности проектирования оптимальной системы защиты информации

Целью построения СЗИ является минимизация информационных рисков для объектов защиты. В качестве целевой функции защищенности, характеризующей риск для информационных ресурсов, примем *относительный потенциальный ущерб* E (12), характеризующий потенциальный ущерб от воздействия совокупности выявленных источников угроз, угроз и уязвимостей объектов защиты с учётом затрат, связанных с использованием СЗИ. Однако, создание в ИС дополнительной подсистемы, решающей задачу защиты информации, приводит к уменьшению её функциональности (ограничение функций ИС, для которых невозможно или затруднительно создать механизм защиты) и производительности (увеличение времени доступа к защищаемым объектам). Эту ситуацию можно наглядно показать треугольником противоречий трёх показателей (рис. 5).

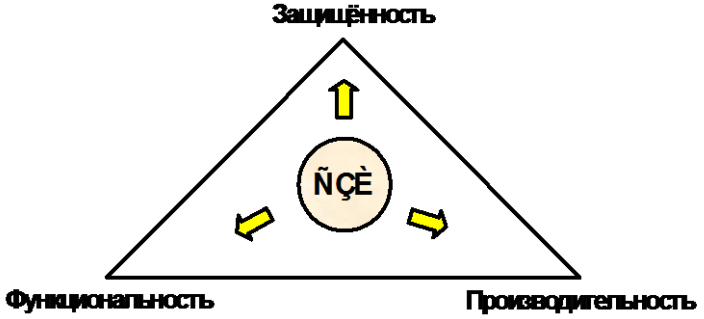

Рисунок 5 – Зависимость защищенности, функциональности, производительности от мощности СЗИ

Защищенность ИС Z можно представить как функцию, зависящую от относительного потенциального ущерба при реализации угроз, функциональности и производительности ИС:

$$Z = f(E, N_f, T_a), \tag{14}$$

где E – относительный потенциальный ущерб при реализации угроз, N_f – количество функций, характеризующих функциональность ИС, T_a – среднее время доступа к объектам защиты ИС.

С учётом этого задача оптимизации заключается в обеспечении максимального уровня защищённости при минимальном относительном потенциальном ущербе, максимальной функциональности и производительности ИС (максимум функций ИС и минимум среднего времени доступа к объектам защиты ИС):

$$Z_{max}\begin{cases} E \to min; \\ N_f \to max; \\ T_a \to min. \end{cases} \tag{15}$$

Такая постановка свидетельствует о многокритериальном характере задачи проектирования СЗИ, что естественно усложняет её решение. Поэтому задачу целесообразно свести к однокритериальной путём введения ограничений. В результате получим

$$Z_{opt}\begin{cases} E \to min; \\ N_f \geq N_{f0}; \\ T_a \leq T_{a0}. \end{cases} \tag{16}$$

где N_{f0} и T_{a0} - заданные ограничения на функциональность и производительность ИС.

С практической точки зрения удобнее оперировать не требуемой функциональностью и производительностью, а снижением функциональности (ΔN_f) и производительности (ΔT_a) от установки системы защиты. Тогда однокритериальная задача оптимизации будет выглядеть следующим образом:

$$Z_{opt}\begin{cases} E \to min; \\ \Delta N_f \geq \Delta N_{f0}; \\ \Delta T_a \leq \Delta T_{a0}. \end{cases} \quad (17)$$

где ΔN_{f0} и ΔT_{a0} - заданные ограничения на снижение функциональности и производительности ИС.

Если рассчитанное значение относительного потенциального ущерба E не удовлетворяет требованиям к эффективности СЗИ, то в допустимых пределах можно изменять заданные ограничения на снижение функциональности и производительности, решая задачу оптимизации методом последовательного снижения ограничений. При этом необходимо задать шаг снижения функциональности и производительности.

В этом случае задача решается путем реализации итерационной процедуры с отсеиванием вариантов, не удовлетворяющих заданному относительному потенциальному ущербу, и снижением требований к ограничениям по функциональности и производительности.

Особенностью проектирования СЗИ является то, что исходные данные, полученные на первых этапах построения СЗИ, изменяются с течением времени функционирования ИС, что может быть связано с изменением условий и среды функционирования, потерей или увеличением стоимости информационных ресурсов, нахождением злоумышленниками ошибок в реализации методов и средств защиты. Эти изменения должны быть учтены в процессе функционирования СЗИ. Поэтому процедура проектирования СЗИ также является итерационной.

Последовательность задач, решаемых при проектировании СЗИ, можно представить следующим образом.

1. Расчёт параметров N_f и T_a.
2. Назначение ограничений ΔN_{f0} и ΔT_{a0}.
3. Анализ векторов S, A, V, R (рис. 3).
4. Формирование нескольких вариантов векторов C (вариантов СЗИ), отличающихся стоимостью реализации.
5. Расчет результатов преобразований $S \xrightarrow{C} S^c$, $A \xrightarrow{C} A^c \xrightarrow{S^c} A^{cs}$ $V \xrightarrow{C} V^c \xrightarrow{A^{cs}} V^{csa}$ для всех вариантов C.
6. Расчёт E, ΔN_f и ΔT_a для всех вариантов C.
7. Выбор системы защиты информации с минимальным E, удовлетворяющей условиям $\Delta N_f \geq \Delta N_{f0}$, $\Delta T_a \leq \Delta T_{a0}$.
8. Если варианты СЗИ не удовлетворяют заданным ограничениям, то проведение анализа изменения E при задании приращений ΔN_{f0} и ΔT_{a0} методом последовательного снижения ограничений с оценкой целесообразности выбора СЗИ, удовлетворяющей новым ограничениям.

При формировании СЗИ необходимо учитывать, что любой механизм защиты должен проектироваться с учётом его влияния в целом на безопасность ИС и с учётом функций других механизмов защиты. Комплексирование разнородных механизмов защиты в единую систему повышает качество и эффективность функционирования СЗИ.

VII Заключение

Предложенный метод проектирования оптимальной СЗИ должен быть обеспечен проверенным и обоснованным методом экспертных оценок. С целью проверки эффективности и состоятельности, а также для практического использования предложенного метода необходимо создание программного инструментария, которое могло бы рассматриваться как автоматизированное рабочее место по созданию СЗИ. После получения позитивного опыта при реализации предложенного метода проектирования оптимальной СЗИ можно говорить о его нормативном закреплении либо в целом, либо отдельных его положений.

Литература: ***1.*** *Воронцов Ю. В., Гайдамакин Н. А. Модель комплексной оценки защищенности компьютерных систем в идеологии ущерба от угроз безопасности. "Вопросы защиты информации", №1, 2003 г.* ***2.*** *Вихорев С. В., Кобцев Р. Ю. Как узнать – откуда напасть или откуда исходит угроза безопасности информации. Журнал "Защита информации. Конфидент", №2, 2003.*

УДК 681.3

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ ВЕРОЯТНОСТНЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ РЕШЕНИЯ ЗАДАЧИ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ КОМПЬЮТЕРНЫХ СИСТЕМ

Елена Высоцкая, Анатолий Давиденко*
Национальный авиационный университет
**Институт проблем моделирования в энергетике им. Г. Е. Пухова НАН Украины*

Аннотация: **Исследуется возможность и эффективность применения вероятностных нейронных сетей для аутентификации пользователя компьютерных систем. Определяются ограничения, которые связанны с областью применения данного подхода. Выделяются наиболее критичные параметры, за счет настройки которых можно повышать эффективность данного метода. Проводится количественный и качественный анализ этих параметров.**

Summary: **In this article the opportunity and efficiency of application of probabilistic neural networks for authentification of the user of computer systems is researched. The limitations are defined, which one are connected with area of applicability of this approach. The most critical parameters are selected, at the owing to of regulation which one are possible are to raise efficiency of this method. The quantitative and qualitative analysis of these parameters will be carried out.**

Ключевые слова: **Вероятностные нейронные сети, аутентификация пользователя, классификация, распознавание образов, защита информации.**

Одной из наиболее часто встречающихся угроз является угроза несанкционированного доступа к компьютерной системе пользователей, которые являются сотрудниками организации или имеют временный доступ к системе. Одним из способов решения этой проблемы является аутентификация пользователя компьютерной системы. Поэтому можно сказать, что одной из главных задач защиты информации [1 – 3] является задача аутентификации пользователей компьютерных систем. В результате рассмотрения основных способов аутентификации был выбран механизм, который использует особенности работы пользователя на клавиатуре, т. е. “почерк” пользователя. При этом задачу аутентификации можно свести к задаче классификации или распознавания образов. Одним из наиболее эффективных механизмов для решения этих задач являются механизмы на базе нейронных сетей [4 – 11]. В результате анализа особенностей основных видов нейронных сетей [4 – 6], были выбраны вероятностные нейронные сети (сеть PNN – Probabilistic Neural Network) [4].

Цель данной работы:

1. исследовать возможность применения вероятностных нейронных сетей для аутентификации пользователя компьютерных систем;
2. определить эффективность использования вероятностных нейронных сетей для решения выбранной задачи;
3. определить ограничения, которые связанны с областью применения данного подхода;
4. выделить наиболее критичные параметры, за счет настройки которых можно повышать эффективность данного метода;
5. провести количественный и качественный анализ наиболее критичных параметров.

Для достижения поставленной задачи была создана на языке Borland C++ Builder программа на базе вероятностной нейронной сети для определения эффективности применения данного вида нейронных сетей для решения задачи аутентификации пользователей компьютерной системы. Для обработки и хранения информации использовалась программа для работы с базами данных Database Desktop 7.0 и SQL-запросы. Затем, с помощью созданной программы была накоплена информация о “почерке” работы на клавиатуре некоторого количества пользователей, после чего, на основе этих данных было проведено ряд экспериментов.