УДК 004.056

МОДЕЛЬ ВЫБОРА ОПТИМАЛЬНОГО СОСТАВА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Петров А.А.

MODEL OF THE OPTIMAL CHOICE OF INFORMATION SYSTEMS IN COMPUTER NETWORKS

Petrov A.

В статье представлены результаты исследований по разработке методологии организационно-технического управления защиты информации (ЗИ), включающей соответствующие модели и методы принятия решений, организации контроля уровня защищенности (риска). На основании разработанных методов и моделей могут быть сделаны предложения по модернизации и совершенствованию систем защиты информации (СЗИ), они могут использоваться при проектировании СЗИ и в процессе её эксплуатации.

Ключевые слова: *защита информации, системы защиты информации, модель защиты, морфологиечский метод.*

Введение

Для совершенствования, развития и повышения эффективности СЗИ необходима разработка и практическое применение методического обеспечения, связанного с решением следующих частных задач проектирования системы и управления защитой информации [1-7]:

- разработка модели СЗИ – получение описания организованной совокупности программно-аппаратных средств защиты, как можно более полно учитывающей потенциально возможные источники угроз;
- разработка математического метода формирования рационального комплекса средств защиты, который позволяет повысить степень научной обоснованности выбора и учесть требования, предъявляемые к механизмам защиты при обработке информации ограниченного доступа; процедура синтеза наборов СЗ должна обеспечить выбор рационального состава СЗИ, который в комплексе обеспечивает требуемое значение уровня защищенности информации на объекте защиты;
- поскольку требуемый уровень защищенности зависит от максимального уровня критичности обрабатываемой в данный период времени на объекте защиты информации, необходимо обоснование рациональных наборов СЗ при изменении планов обработки информации в компьютерной информационной системе (КИС);
- синтез структуры и алгоритмов функционирования системы поддержки принятия решений (СППР) для системы управления ЗИ;
- оценивание ожидаемого значения относительного риска и уровня защищенности информации на объекте защиты.

Рассмотрим процесс построения многорубежной модели СЗИ на основе базовых принципов построения системы защиты.

Модель защиты – формализованное или неформализованное описание комплекса программно-аппаратных средств и организационных мер защиты, являющееся основой для разработки системы защиты информации [2].

В [3] отмечается необходимость максимальной структуризации изучаемых систем и разрабатываемых решений. Структуризация может быть определена как процесс формирования такой архитектуры разрабатываемой системы, которая наилучшим образом удовлетворяет всей совокупности условий ее разработки, эксплуатации и усовершенствования.

Кроме того, если рассматривать КИС как интеграцию рабочих станций, серверов, межсетевых мостов, аппаратуры и каналов связи, то при создании СЗИ следует использовать следующие ключевые принципы ее построения, которые обобщают основные положения современной концепции ЗИ [2]:

- комплексность и согласованность использования широкого спектра методов и средств защиты при построении целостной системы защиты, не содержащей слабых мест на стыках ее компонентов;
- дифференциация мер защиты в зависимости от критичности (важности) информации и потенциально возможных угроз информационным ресурсам;

- разумная достаточность механизмов защиты, что означает правильность выбора достаточного уровня защиты, при котором затраты на СЗИ и размер возможного ущерба (риск) были бы приемлемыми.

На основе анализа всех возможных каналов несанкционированного доступа к информационной среде КИС и в соответствии с приведенными выше основными принципами построения системы защиты предлагается многорубежная модель СЗИ.

Первый рубеж – периметр объекта защиты – набор функциональных подсистем, включающих средства и механизмы системной защиты от внешних угроз злоумышленника и потенциально возможных деструктивных воздействий удаленного пользователя; второй рубеж — набор функциональных подсистем защиты сетевого сегмента от потенциально возможных межсегментных и удаленных атак; третий рубеж включает в себя набор функциональных подсистем, обеспечивающих защиту информационной среды отдельного персонального компьютера, сервера.

В [4] отмечается, что гибридные атаки, использующие множество стратегий нападения, могут быть остановлены только многоуровневой, эшелонированной линией обороны.

Таким образом, модель СЗИ включает в себя три компонента: модель защиты периметра объекта защиты, модель защиты сетевого сегмента, модель защиты ПК и сервера.

Модель каждого рубежа защиты является N-уровневой и включает в себя N морфологических матриц, в зависимости от уровня критичности (важности) обрабатываемой на объекте защиты информации.

Такое организованное системное упорядочение информации является средством её предметной организации, обеспечивающим процесс использования информации о возможных угрозах информационной среде и соответствующих им необходимых барьерах, которое уменьшает уровень неопределенности при принятии решения о составе СЗИ.

Схематично многорубежная модель СЗИ для N=3 приведена на рис. 1.

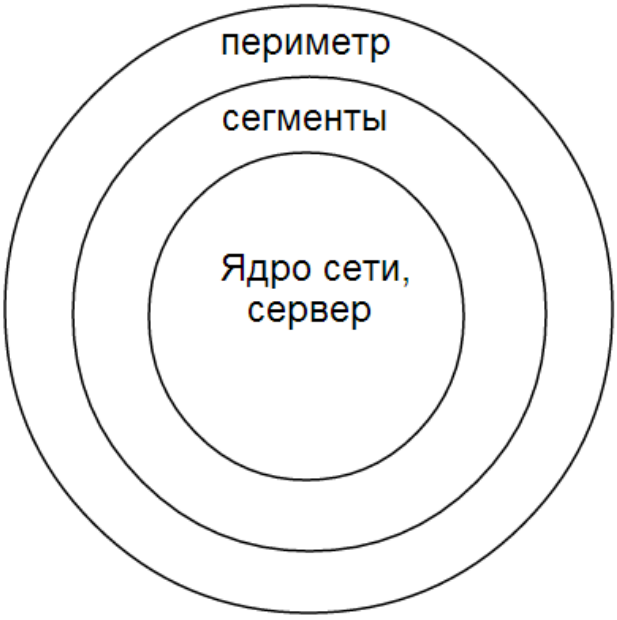

Рис. 1. Трехрубежная система защиты компьютерной сети

Назначение данной модели – получить от пользователя информацию о его предпочтениях и, используя определенные процедуры, упорядочить сравниваемые альтернативные реализации барьеров путем многокритериального сравнительного анализа информации о средствах защиты. Это позволит выявить в заданном множестве возможных реализаций набора СЗ для рубежа подмножество наилучших по критериям предпочтения вариантов анализируемого объекта исследования.

Приведем обоснование целесо-образности применения морфологического подхода к формированию рациональных наборов средств защиты для рубежей защиты.

Развитие и совершенствование методологии проектирования систем защиты информации и повышения эффективности их функционирования предполагает получение количественных методов анализа и синтеза систем защиты и управление СЗИ в процессе функционирования.

В работе используется идея морфологического подхода для моделирования и синтеза рациональных наборов средств защиты в СЗИ.

Впервые в систематизированном виде морфологический подход был разработан и применен швейцарским астрономом Ф. Цвикки. Основная идея морфологического метода – систематизировать нахождение всех мыслимых вариантов решения проблемы путем комбинирования выделенных элементов морфологической таблицы (матрицы) [5]. Морфологический метод является аппаратом анализа и синтеза, который применяется в различных областях знаний. Сущность его заключается в том, что в результате морфологического анализа определяется морфологическое множество, которое обязательно включает в себя искомое решение. Затем пространство поиска сужается — осуществляется поиск наилучшего элемента морфологического множества. Использование морфологического метода для выбора рациональных вариантов становится возможным после дополнения его экспертными знаниями для независимого оценивания функциональных подсистем, позволяющими проводить выбор.

Морфологический метод синтеза целесообразно использовать при проектировании СЗИ и в процессе организационно-технического управления ЗИ, поскольку метод позволяет реализовать многоальтернативный и многокритериальный выбор, когда система представляет собой сложный комплекс СЗ, включающий в себя наборы средств защиты для определенных точек их установки на объекте защиты; каждый набор синтезируется из некоторого множества функциональных подсистем защиты, и каждая имеет более одного альтернативного средства защиты для её реализации.

Применительно к проблеме выбора рациональных наборов средств защиты для рубежей морфологический метод состоит в том, чтобы для каждого рубежа защиты определить все необходимые функциональные подсистемы в соответствии с требованиями защиты, от которых зависит решение проблемы синтеза; представить их в виде матриц-строк, включающих в качестве элементов альтернативные средства защиты, а затем определить в этой морфологической матрице все возможные сочетания средств защиты по одному из каждой строки.

Полученные таким образом варианты наборов средств защиты подвергаются анализу и оцениванию в целях выбора наилучшего набора СЗ. Такие наборы называются вариантами решения задачи синтеза, или альтернативами.

Рассмотрим построение модели рубежа защиты.

Морфологическая матрица альтернатив для выбора набора средств защиты рубежа составляется с учетом сформулированных на основе стандартов и нормативных документов требований и может быть представлена в табличной форме (таблица 1).

Таблица 1

Морфологическая матрица средств защиты рубежа

Функциональные подсистемы	Требования к средствам защиты	Альтернативные средства защиты	Количество СЗ
$Ф_1$	$T_{11} - T_{1n_1}$	$A_{11}\ A_{12}\ \dots\ A_{1i}\ \dots\ A_{1k_1}$	K_1
$Ф_2$	$T_{21} - T_{2n_2}$	$A_{21}\ A_{22}\ \dots\ A_{2j}\ \dots\ A_{2k_2}$	K_2
…		…	…
$Ф_l$		$A_{l1}\ A_{l2}\ \dots\ A_{lm}\ \dots\ A_{lk_l}$	K_l
...	...	...	...
$Ф_L$	$T_{Ll} - T_{ln_l}$	$A_{L1}\ A_{L2}\ \dots\ A_{Ln}\ \dots\ A_{Lk_L}$	K_L

Для каждого рубежа защиты, таким образом, создается N различных морфологических матриц, в которых отражаются L функциональных подсистем для рубежа. Задаются требования к каждой функциональной подсистеме в зависимости от уровня критичности информации. Альтернативные реализации средств защиты для каждой функциональной подсистемы рубежа определяются с учетом этих требований.

Элементы морфологической матрицы - средства защиты. Общее число возможных вариантов решения проблемы, содержащихся в морфологической матрице, равно

$$R = K_1 \bullet \dots K_l \bullet \dots K_L, \qquad (1)$$

где L – число строк морфологической таблицы, или число функциональных подсистем; K_l – число альтернативных средств защиты в l-ой строке.

После построения матрицы для рубежа защиты приступают к определению функциональной ценности каждого средства защиты и издержек от их использования.

Наиболее предпочтительным для оценки СЗ является критериальный метод, когда каждое отдельно взятое средство защиты оценивается конкретным числом. При практическом рассмотрении средств защиты выясняется, что для их оценивания требуется некоторое множество критериев, причем в большинстве случаев невозможно найти СЗ, являющееся предпочтительным на всем множестве критериев. При оценке СЗ нужно различать качество средства защиты и эффективность реализуемых им процессов.

Качество – это совокупность атрибутивных свойств, существенных для использования СЗ по назначению. Показатель качества СЗ - вектор показателей существенных свойств, характеризующих пригодность СЗ для использования по назначению. Каждое i-е качество l-го СЗ $\{K_{il}\}$, может быть описано с помощью переменной, отображающей определенное существенное свойство СЗ, значение которой характеризует меру этого качества.

Эту меру назовем частным показателем качества СЗ. Показатель может принимать значения из множества (области) допустимых значений. Обобщенным показателям качества l-го СЗ назовем вектор, компоненты которого суть показатели его отдельных свойств. Размерность этого вектора определяется числом существенных свойств СЗ. Частные показатели качества имеют различную физическую природу и различную размерность. Выявление совокупности частных показателей качества средств защиты каждой функциональной подсистемы для проведения сравнительного анализа и обоснования выбора СЗ для эксплуатации в конкретной СЗИ является одной из задач, решаемых при выборе рациональных наборов средств защиты.

Дадим формализованное описание процесса планирования рационального модульного состава СЗИ.

Планирование ЗИ как функция управления в процессе управления СЗИ представляет собой процесс последовательного снятия неопределенности относительно структуры СЗИ и состава средств защиты на объекте управления. В первую очередь необходимо сформулировать перечень требований и получить характеристики требуемого состояния объекта управления. Исходя, из целевого назначения объекта управления требуемое состояние СЗИ можно оценить значением уровня защищенности (риска). На первом этапе необходимо сформировать структуру СЗИ и задать диапазон изменения выходной управляемой переменной. На втором этапе реализуется выбор способа достижения планируемого, требуемого уровня защищенности. В [7] приведено выражение, описывающее структуру процесса планирования

$$P_{пл} = \langle I, F \rangle \qquad (2)$$

где I - информационный компонент, описывающий сведения, используемые для получения текущего решения в форме задачи принятия решений; F – процедурный компонент, включающий основные функции принятия решений (обмен информацией, расчетные, эвристические процедуры, основанные на неформальных правилах экспертов).

В ходе планирования реализуются функции содержательного преобразования информации. Процесс планирования рациональных наборов СЗ характеризуется с помощью выражения.

$$P_{пл} = \Phi \to S_r \qquad (3)$$

В каждом процессе планирования процедуры порождения альтернатив и использования правила выбора наилучшей альтернативы (набора СЗ) образуют механизм получения решения. Множество функциональных подсистем для рубежей защиты задается на первом этапе, результатом процесса планирования является командная информация, которая содержит конкретные данные по распределяемым ресурсам, направляемым на достижение целевого состояния ОУ.

Процесс принятия решения о выборе рационального варианта набора СЗ для рубежа защиты — это функция преобразования содержания информации о требованиях, предъявляемых к средствам защиты определенных функциональных подсистем, входящих в набор, о характеристиках средств защиты, в подмножество наилучших вариантов набора $S' \subseteq S$.

Множество вариантов набора

$$S = \{S_1, \ldots, S_r, \ldots, S_R\}, \qquad (4)$$

где R – число вариантов альтернатив, из которых осуществляется выбор.

Обозначим целевую функцию – принцип выбора, по которому осуществляется выбор рационального набора СЗ, через J. Тогда множество выбранных альтернатив, в частности одна,

$$S_r = J(S) \qquad (5)$$

В задачах принятия решений используют понятие механизма выбора, который представляет собой кортеж из двух элементов: совокупность сведений, позволяющих сопоставлять варианты или группы вариантов, и правило выбора, указывающее, как, использую структуру сведений, выделить из предъявленного

для выбора множества альтернатив S подмножество S' или одну альтернативу S_r.

Обозначим общую совокупность сведений о средствах защиты функциональных подсистем рубежа, позволяющих задавать бинарные отношения сходства, отношения предпочтения, превосходства, через совокупность сведений о СЗ l-ой функциональной подсистемы, позволяющих задавать те же отношения, - через W.

Для средств защиты l-ой функциональной подсистемы множество W_l включает в себя два подмножества:

$$W_{\text{зщ}l} \subset W_l \text{ и } W_{\text{и}} \subset W_l, \quad (6)$$

где $W_{\text{зщl}}$ – показатель «защищенности»; $W_{\text{иl}}$ – показатель «издержки» средства защиты для l-ой функциональной подсистемы.

При использовании морфологического метода синтеза модель ПР можно представить в следующем виде:

$$\text{ПР}: \langle \text{Ц}, \Phi, \Pi_S, S, W_l, J, S_r(S') \rangle \quad (7)$$

где Ц – цель принятия решения; Ф – исходные данные для порождения альтернатив (множество функциональных подсистем для рубежа защиты); Π_s – правило порождения альтернатив; S – множество порожденных альтернатив; W_l – данные для выбора рациональных вариантов: множество характеристик защищенности и издержек средств защиты для каждой l-ой функциональной подсистемы; J – правило выбора наилучшей альтернативы; S_r – выбранная альтернатива.

$$\Phi = \{\Phi 1, \Phi 2, ..., \Phi l, ..., \Phi L\} \quad (8)$$

Правило порождения альтернатив Π_s может быть представлено в аналитическом виде как векторное произведение множеств

$$S = \Phi_1 \times \Phi_2 \times \ldots \times \Phi_l \times \ldots \times \Phi_L, \quad (9)$$

где Φ_l – обозначение l-ой функциональной подсистемы; Φ_l – множество, состоящее из средств защиты для данной подсистемы;

$$\Phi_l = \{A_{l1}, A_{12}, ... A_{1т} ..., A_{lkl}\} \quad (10)$$

Графически структура задачи принятия решений, обеспечивающая преобразование исходных данных в решение по выбору рационального варианта набора СЗ для рубежа, может быть представлена в виде последовательности правил порождения альтернатив и выбора наилучшей по заданной целевой функции, приведенном на рис. 2.

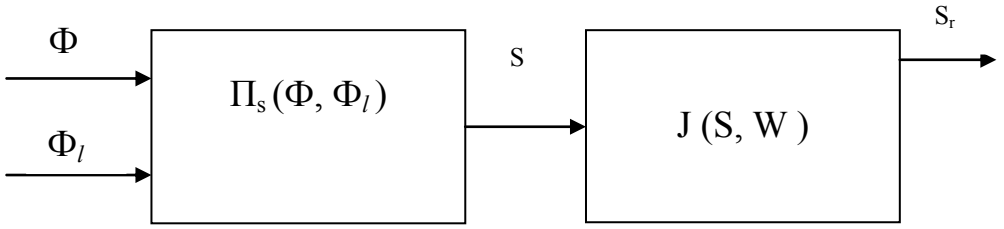

Рис. 2. Структура задачи принятия решений по выбору рационального варианта набора СЗ для рубежа защиты

Выводы

Задача принятия решений по выбору рационального варианта набора СЗ требует для своего решения разработки метода обработки знаний, который использует неформализуемый опыт специалистов - экспертов в области защиты информации. Такой метод должен обеспечивать преобразование данных из базы знаний и вывод решений в аналитической форме.

Следует отменить, что в условиях автоматизированного управления и при использовании экспертной информации в процессе принятия решения можно говорить (даже в случае формализованного правила выбора) о рациональном, а не оптимальном решении. В этом случае для решения задач используются аналитические методы, позволяющие осуществлять многокритериальный выбор, однако получаемые решения зависят от субъективных мнений лица, принимающего решение.

Литература

1. Петров А.А. Разграничение доступа к информации в компьютерных сетях / Петров А.С., Хорошко В.А. // Інформаційна безпека: науковий журнал. – 2010. - № 1(3). – С. 31-38.

2. Рахимов // Информационные технологии . - 2006. - № 10. - С. 17-26.

3. Домарев, В. В. Безопасность информационных технологий. Системный подход. - Киев: ООО ТИД ДС, 2004. - 992 с.

4. Малюк, А. А. Информационная безопасность и методологические основы защиты информации: учеб. пособие для вузов / Малюк А. А. — М: Горячая линия — Телеком, 2005. - 280 с.

5. Лукацкий, А. В. Обнаружение атак. — СПб.: БХВ - Петербург, 2003. - 608 с.

6. Zwicky, F. Discovery, Invention, Research through the Morphological Approach. - New York : McMillan, 1969.

7. Машкина, И. В. Проектирование системы защиты информации объекта информатизации / И. В. Машкина, В. И. Васильев, Е. А.

References

1. Petrov A.A. Razgranichenie dostupa k informacii v komp'juternyh setjah / Petrov A.S., Horoshko V.A. // Informacijna bezpeka: naukovij zhurnal. – 2010. - № 1(3). – S. 31-38.
2. Rahimov // Informacionnye tehnologii . - 2006. - № 10. - S. 17-26.
3. Domarev, V. V. Bezopasnost' informacionnyh tehnologij. Sistemnyj podhod. - Kiev: OOO TID DS, 2004. - 992 s.
4. Maljuk, A. A. Informacionnaja bezopasnost' i metodologicheskie osnovy zashhity informacii: ucheb. posobie dlja vuzov / Maljuk A. A. — M: Gorjachaja linija — Telekom, 2005. - 280 s.
5. Lukackij, A. V. Obnaruzhenie atak. — SPb.: BHV - Peterburg, 2003. - 608 s.
6. Zwicky, F. Discovery, Invention, Research through the Morphological Approach. - New York : McMillan, 1969.
7. Mashkina, I. V. Proektirovanie sistemy zashhity informacii ob#ekta informatizacii / I. V. Mashkina, V. I. Vasil'ev, E. A.

Petrov A.A.

MODEL OF THE OPTIMAL CHOICE OF INFORMATION SYSTEMS IN COMPUTER NETWORKS

The article presents the results of research to develop the methodology of organizational and technical management of information security, which includes the relevant models and methods of decision-making, organizations control the level of security (risk). On the basis of the developed methods and models can be made proposals for the modernization and improvement of information security systems (ISS), they can be used in design and ISS in the course of its operation.

Keywords: information security, information security systems, security model, morphological method.

Петров А.А.

МОДЕЛЬ ВИБОРУ ОПТИМАЛЬНОГО СКЛАДУ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

У статті представлені результати досліджень з розробки методології організаційно-технічного управління захисту інформації (ЗІ), що включає відповідні моделі і методи прийняття рішень, організації контролю рівня захищеності (ризику). На підставі розроблених методів і моделей можуть бути зроблені пропозиції щодо модернізації та вдосконалення систем захисту інформації (СЗІ), вони можуть використовуватися при проектуванні СЗІ і в процесі її експлуатації.

Ключові слова: *захист інформації, системи захисту інформації, модель захисту, морфологічний метод.*

Петров Антон Александрович – кандидат технических наук, доцент, ВНУ им. В. Даля.

Рецензент: Петров Олександр Степанович – докт. техн. наук, професор, завідувач кафедри безпеки інформаційних систем, Східноукраїнський національний університет імені Володимира Даля, м. Луганськ.