КОМП'ЮТЕРНІ ЗАСОБИ, МЕРЕЖІ ТА СИСТЕМИ

УДК.681.322.00; 681.324.00; 004.056.5

А.В. ПАЛАГИН, Ю.С. ЯКОВЛЕВ, Б.М. ТИХОНОВ

ПАРАДИГМА ПОСТРОЕНИЯ ИНФОРМАЦИОННОЙ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СИСТЕМ В ЗАВИСИМОСТИ ОТ СТЕПЕНИ ВАЖНОСТИ ИНФОРМАЦИИ

Предлагается парадигма построения подсистемы защиты, которая основана на взаимосвязи между важностью информации и набором средств для построения подсистемы защиты требуемого уровня. При этом учитываются архитектурно – структурная организация среды, в которой работает пользователь (отдельный компьютер, локальная или корпоративная сеть), а также некоторые критерии оптимизации (например, стоимость, производительность и др.).

Введение. В настоящее время начинает доминировать тенденция расширения применения компьютерных систем (КС) на те сферы человеческой деятельности, где необходимо хранить и обрабатывать конфиденциальную информацию.

Существует большое количество средств и методов информационной защиты [1– 6], и даже соответствующие стандарты, позволяющие выбрать тот или иной уровень защиты, который, как правило, диктуется больше субъективными факторами, нежели объективными. В компьютерных системах, применение которых связано с использованием информации различной степени важности, целесообразно подходить к построению подсистемы информационной защиты рационально, не загромождая её дорогими и часто недостаточно эффективными аппаратными и программными средствами. Не вызывает сомнений, что всякую информацию и решаемые задачи можно оценить с точки зрения их важности через совокупность так называемых информационных категорий, которые могут быть интерпретированы как относительные показатели уровней информационной защиты. Кроме того, среди существующих в настоящее время многочисленных средств защиты всегда можно выделить отдельные группы (например, по совокупности функций, значениям параметров и результатам практического применения различными фирмами), которые обеспечивают

определенные уровни информационной защиты. Таким образом, существует реальная возможность установить взаимосвязь между важностью информации и набором средств, необходимых для построения подсистемы защиты требуемого уровня, а также создать соответствующую методику их выбора. Несмотря на многочисленные публикации по проблеме защиты информации, такой подход к построению подсистем защиты авторам неизвестен.

Степень важности информации определяется прежде всего тем, какой смысл в неё заложен и насколько эта информация для соответствующих категорий пользователей является ценной с различных точек зрения: экономической, социальной, политической и т.д. При этом большое значение приобретает проблема информационного взаимодействия, главными составляющими которой являются человеко-машинный интерфейс и языковые аспекты [7], особенно, когда речь идет о массовом интеллектуальном информационном сервисе [8], параллельно с которым бурно развиваются технологии и средства добычи знаний, например, технология KDD (Knowledge Discovery in Data base – обнаружение знаний в базах данных) [9].

Предлагая новую парадигму построения подсистем информационной защиты, рассмотрим категорию важности информации с точки зрения её информационной емкости и ценности для административно-структурных подразделений различного уровня. Основные положения подхода достаточно общие и могут быть использованы при решении всей совокупности вышеотмеченных проблем.

Основные положения подхода. Вполне очевидно, что для пользователей любой системы информационной поддержки вся информация (INF) с точки зрения информационной емкости может быть представлена следующими категориями: данные (D), метаданные (MD) и знания (Zn) о конкретной предметной области, $(INF) \subset (D, MD, Zn)$. Высшую категорию ценности представляют собой знания, поскольку они являются продуктом различных технологий интеллектуального анализа, обработки и структурирования данных и дают наиболее полное представление о предметной области, включая субъекты, объекты и процессы.

Следующую категорию по степени важности представляют метаданные или данные о данных, поскольку метаданные – информация о том, что представляют собой данные, их основные типы, элементы и структура, процессы преобразования, где хранятся данные, как получить доступ к ним и т.д. [10]. Доступ к метаданным, как правило, имеют все программы, обслуживающие и использующие базы данных (БД). Они весьма привлекательные для несанкционированных пользователей.

И, наконец, степень важности данных можно расценивать с точки зрения возможности получения на их основе новых знаний, при этом интерес к таким данным определяется тем, к какой из нижеобозначенных категорий они относятся и в каком виде представлены (структурированные, полуструктурированные и т.д.) [11] .

Можно выделить несколько категорий информации (INF) исходя из принадлежности к соответствующему уровню организационно–структурной иерархии: государственного значения $(INF)_Г$, отраслевого – $(INF)_{ОТ,}$ регионального – $(INF)_{РГ}$, предприятия – $(INF)_{ПП}$, подразделения – $(INF)_{ПД}$ и т.д. Для каждой из этих категорий могут быть определены соответствующие уровни доступности (секретности) информации, например: особо важная (совершенно секретная – СС), секретная – С, для служебного пользования – СП, без какого либо грифа важности (секретности) – БГ и т.д. При этом для каждого уровня доступности по массовости использования и адресному назначению можно выделить следующую информацию: целевого ограниченного назначения – ЦН (например, для одного человека – только для сетевого диспетчера, руководителя министерства, ведомства и т.д.); группового назначения – ГР (например, для конкретной категории пользователей); общего назначения – ОН (например, для всех пользователей корпоративной сети) и т.д.

Как правило, информация, относящаяся к соответствующему уровню, приоритеты уровней и степень доступа конкретных пользователей, а также групп пользователей к информации конкретной категории определяются соответствующими службами и закрепляются специальными документами (например, приказами, постановлениями, отраслевыми стандартами и даже ГОСТами).

Совокупность вышерассмотренных категорий можно отобразить с помощью схемы, общий вид которой для принятой иерархической последовательности критериев показан на рис. 1, при этом фрагмент дерева, отражающий взаимосвязь некоторых категорий (согласно рис. 1), изображен на рис. 2. Используя схему типа рис. 2, можно дать относительную оценку важности информации (и соответственно требуемую относительную степень защищенности) для заданного набора информационных категорий, составляющих одну из ветвей дерева категорий. Например, можно отметить, что при прохождении по крайней левой ветви дерева рис. 2 получим наивысшую степень важности информации $G(INF)_{max}$, требующую соответственно самую высокую степень её защиты. В данной систематике обозначений $G(INF)_{max}$ может быть отображена как

$$G(INF)_{max} \supset [(INF), (Zn), (INF)_Г , СС, ЦН],$$

что означает: информация, представленная в виде новых знаний, имеет гриф секретности СС и предназначена только для одного пользователя (например, руководителя министерства).

Для сравнительной оценки степени важности информации, циркулирующей в системе, которая отображена соответствующей ветвью дерева информационных категорий, необходимо выполнить количественную оценку каждой выделенной категории каждого уровня, используя при этом так называемые коэффициенты важности.

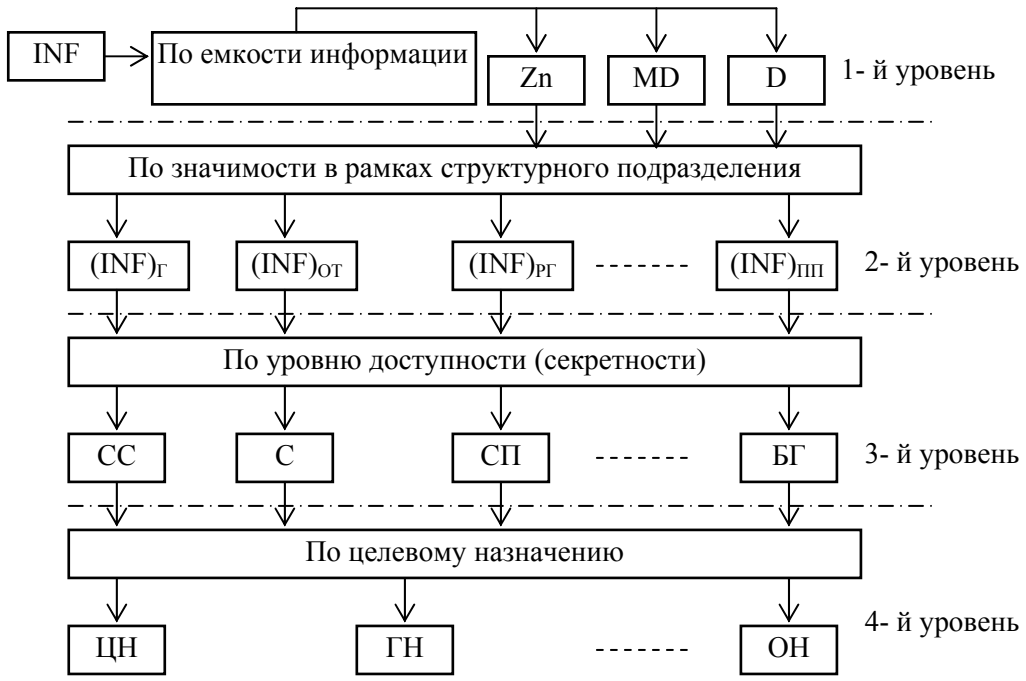

РИС. 1. Информационные категории и их приоритетность по уровням

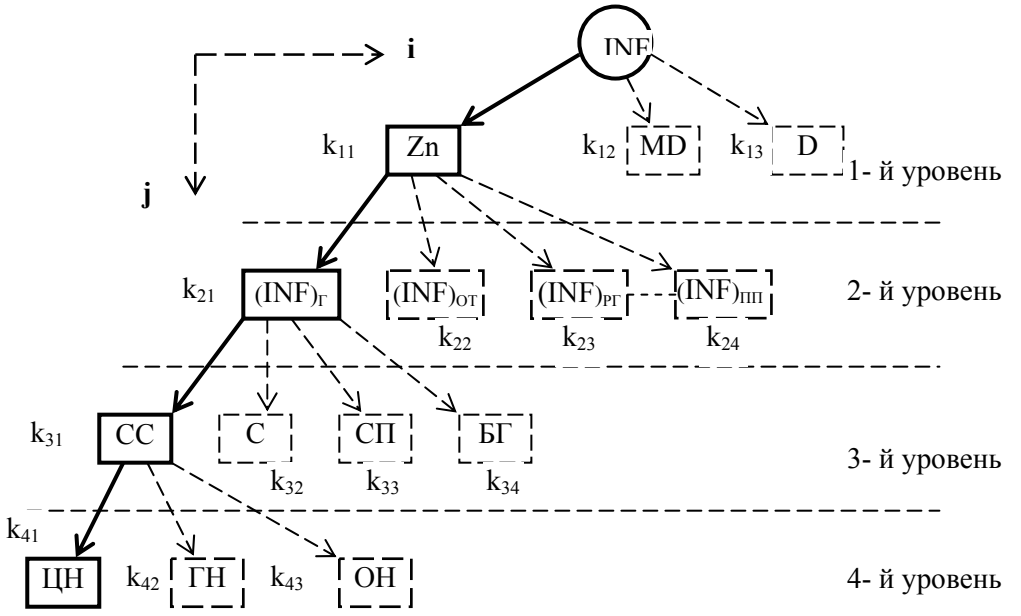

РИС. 2. Часть дерева, отображающая взаимосвязь некоторых информационных категорий

Пусть схема информационных категорий содержит j уровней (j = 1, 2,..., m), а в каждый j - й уровень входит n_j информационных категорий, так что k_{ji} представляет коэффициент важности i - й категории j - го уровня (i = 1, 2, ..., n_j). Для каждого уровня на основе экспертных оценок (либо назначенных директивно соответствующими службами) принимаются значения параметров k_{ji} (при этом $k_{ji} \le 1$). Категория наивысшего приоритета оценивается значением параметра $k_{ji} = 1$. Аналогично оценивается весовой коэффициент P_j каждого уровня ($P_j \le 1$), так что взвешенная степень важности g_{ji} каждой информационной категории оценивается безразмерной величиной вида

$$g_{ji} = k_{ji} P_j \ . \qquad (1)$$

Тогда эквивалентная степень важности $G(B_s)$ информации, которая хранится и циркулирует в компьютерной системе, определяется как сумма взвешенных коэффициентов $(g_{ji})^*$ для информационных категорий, размешенных на помеченной s-й ветви дерева (s = 1,2,…,q), которое отображает взаимосвязь информационных категорий по уровням, т.е.

$$G(B_S) = \sum_{j^*=1}^{m} (g_{ji})^* \ , \qquad (2)$$

где j принимает значения в пределах от 1 до m только для тех информационных категорий, которые принадлежат помеченной (*) ветви дерева, а $G(B_S) \le m$. Например, для помеченной на рис.2 ветви дерева $B_1 \supset$ [(INF) – (Zn) – $(INF)_Г$ – СС– – ЦН] и значений параметров $P_1 = P_2 = P_3 = P_4 = 1$, а также $k_{11} = 0{,}4$; $k_{21} = 1{,}0$; $k_{31} = 0{,}9$; $k_{41} = 0{,}5$ получим $G(B_1) = 2{,}8$.

Полученные таким образом значения $G(B_S)$ для различных ветвей дерева информационных категорий образуют матрицу важности $M[G(B_S)]$ хранящейся и циркулирующей в системе информации различной информационной емкости, которую также можно рассматривать как матрицу, отображающую относительный уровень защиты данных в соответствии со степенью значимости, доступности и целевого назначения информации. Элементы этой матрицы отображают лишь сравнительные оценки требуемого уровня защиты данных для каждой помеченной ветви дерева по отношению к другим. При этом чем больше значение $G(B_S)$ как элемента этой матрицы, тем более высоким должен быть уровень защиты информации, соответствующей помеченной ветви B_S этого дерева. Однако даже такая сравнительная оценка имеет большое значение для последующего анализа и выбора средств и методов защиты особенно, если номенклатура, количество и приоритетность уровней информационных категорий, их наполнение и степень доступа к информации на различных уровнях классифицировано и закреплено соответствующими актами и документами.

Уровень защиты информации определяется не только важностью информации и применяемыми средствами защиты, но также и тем, в какой информаци-

онной среде работает пользователь: либо на автономном компьютере – персональной ЭВМ (ПЭВМ) с разделением во времени с работой на этом же компьютере другого пользователя, либо в локальной сети одновременно с работой группы пользователей (при взаимодействии с ними через централизованную базу данных или с помощью сетевой файловой системы, или через электронную почту), либо в составе корпоративной сети, например, с клиент-серверной архитектурой со специализацией серверов и повышенными требованиями к надежности функционирования и сохранности данных.

Главное, что в любом случае пользователи решают свои задачи, применяя при этом информационные среды (компьютерные системы), реализующие наборы следующих функций [12]: оперативная и пакетная обработка транзакций (система для обработки транзакций); оперативная аналитическая обработка, а также реализация функций экспертных систем (системы поддержки принятия решений); гипертекстовая обработка, электронное документирование, реализация функций географических информационных систем (информационно-справочные системы); управление документооборотом, автоматизация делопроизводства (офисные системы) и др.

Важнейшие проблемы, которые возникают при работе на любой из этих систем с информацией: решение задач стандартизации данных (их структур и моделей), полученных от различных источников; обеспечение работы с неформализованными данными или данными, не поддающимися структуризации, а также являющимися нечеткими; обеспечение возможности работы с огромными объемами данных, что в свою очередь порождает проблемы хранилищ данных [13 – 15] и др.

Для реализации отмеченных функций каждую из указанных систем можно представить в виде набора интегрированных (по сравнению со стандартными) компонентов, которые имеют непосредственное отношение к обозначенным на рис.1,2 информационным категориям, выполняя при этом следующие функции: взаимодействие с БД, сбор, обработка, документирование, выдача информации и т.д. К таким компонентам могут относиться [12]

средства для извлечения данных из разнородных источников, включая неструктурированную информацию, и их представления – PS (Presentation Services);

СУБД с базой данных – DS (Data Services) для манипулирования данными, определения данных, фиксации и т. п.;

средства для реализации файловых функций – FS (File Services) – дисковых операций чтения и записи данных для СУБД и других компонент;

логика управления данными – DL (Data Logic) для реализации операций с базой данных (SQL-операторы SELECT, UPDATE и INSERT);

логика представления – PL (Presentation Logic) для управления взаимодействием между пользователем и ЭВМ;

прикладная логика – BL (Business or Application Logic) – набор правил для принятия решений, вычислений и операций, которые должно выполнить приложение.

С помощью такой систематики обозначений можно отобразить варианты компьютерных систем, которые характеризуются наборами интегрированных функциональных компонентов, имеющих непосредственное отношение к преобразованию, хранению и выдаче информации, представленной через соответствующие информационные категории. В общем случае конкретную систему можно представить в виде

$$[\text{Тип системы}] \supset \{F^*\}, \quad F^* = \{(A), (B), (C)\}, \quad F^* \subset F, \qquad (3)$$

где $F \supset \{PS, DS, FS, DL, PL, BL\}$, F^* – множество, содержащее наборы вышеобозначенных интегрированных функциональных компонентов, входящих в множество F, которые (для случая клиент - серверной архитектуры) представлены в виде трех подмножеств: подмножество A, содержащее функциональные компоненты клиента; подмножество B, содержащее функциональные компоненты первого сервера; подмножество C, содержащее функциональные компоненты второго сервера. Например, для систем с клиент-серверной архитектурой типа централизованная многотерминальная система (условно обозначим её – ЦМС), система с удаленным доступом к данным на сервере БД – (СУДД), система с удаленным представлением данных и с доступом к Unix-системе – (СУПД) соответственно можно записать:

$$[\text{Арх. ЦМС}] \supset \{(PS), (PL, BL, DL, DS, FS)\};$$
$$[\text{Арх. СУДД}] \supset \{(PS, PL, BL, DL), (DS, FS)\};$$
$$[\text{Арх. СУПД}] \supset \{(PS, L),(BL, DL, DS, FS)\},$$

где содержимое в круглых скобках слева отображает функциональные компоненты клиента, а во вторых – сервера.

Каждому интегрированному функциональному компоненту множества F можно поставить в соответствие вполне определенный набор аппаратных и программных средств, а также (при требованиях к защите информации) конкретные компоненты подсистемы защиты. Известно, что подсистема защиты привносит в КС дополнительные аппаратурные затраты и дополнительное программное обеспечение, что приводит не только к увеличению стоимости КС, но и к уменьшению её производительности, причем тем значительнее, чем выше реализуется её уровень защиты.

Например, пользователю, работающему в сети, чтобы получить данные с помощью штатных программ администрирования, необходимо сначала попасть в компьютер (уровень защиты рабочей станции – $Z_{АРМ}$), потом в сеть (сетевой уровень защиты – $Z_{СЕТЬ}$), потом – на сервер БД (уровень защиты сервера – $Z_{СЕРВ}$)

и лишь при наличии соответствующих прав доступа (уровень защиты СУБД – $Z_{СУБД}$) – к конкретной области памяти (ЗУ), где хранятся необходимые ему данные. Кроме того, для работы с БД через клиентское приложение придется преодолеть еще один барьер - уровень защиты приложений ($Z_{ПРИЛ}$).

В этом случае эквивалентное время доступа к информации в системе увеличивается на время задержки $\Delta T_{ЗАЩ}$ последовательного прохождения через цепочку средств защиты:

$$\Delta T_{ЗАЩ} = T(Z_{АРМ}) + T(Z_{СЕТЬ}) + T(Z_{СЕРВ}) + T(Z_{СУБД}) + T(Z_{ПРИЛ}). \qquad (4)$$

Поэтому, учитывая значительную потерю времени и существенное увеличение затрат на подсистему информационной защиты, целесообразно уже на этапе разработки компьютерной системы оценить эффект, который может быть получен от внедрения конкретного проекта системы безопасности.

В соответствии с изложенным в основу новой парадигмы построения и применения подсистемы защиты информации в КС приняты следующие положения:

1.Уровень информационной защиты находится в прямой зависимости от степени важности информации, хранимой и обрабатываемой в КС, т.е. чем выше степень важности информации, тем выше должен быть уровень её защиты.

2. Структурная организация информационной среды, в которой работает пользователь (автономный компьютер, локальная или глобальная сеть), существенно влияет на выбор средств и способов построения подсистемы информационной защиты КС и поэтому выступает в качестве базиса для оценки основных параметров КС, таких как производительность, стоимость и др.

3. Если в КС размещается и циркулирует информация различной степени важности, при этом к уровню производительности системы предъявляются повышенные требования, то создавать подсистему защиты, ориентируясь на информацию только повышенной важности, нецелесообразно, поскольку это приводит к резкому снижению производительности всей КС. В этом случае предлагается применять подсистему защиты, которая при работе санкционированного пользователя могла бы динамически перестраиваться в зависимости от степени важности используемой им информации. При любых обнаруженных атаках несанкционированного пользователя подсистема защиты выдает пользователю информацию низшей степени важности, либо просто "балластную информационную болванку", выдаваемую, например, с помощью генератора случайных чисел. Алгоритм перестройки подсистемы защиты, принципиально возможен и практически реализуем, тем более что вариантов перестройки, как правило, оказывается незначительно, например, всего три – для случаев использования информации повышенной, средней и низкой степеней важности.

4. Поскольку пользователь непосредственно взаимодействует с информацией при решении любых задач через персональный компьютер, то наибольшее внимание при архитектурно-структурной организации подсистемы защиты сле-

дует уделять методам и средствам взаимодействия пользователя с компьютером в целом и его функциональными компонентами в частности, которые реализуют функции сбора, обработки, хранения и выдачи информации.

5. Так как аппаратные средства защиты информации по сравнению с программными средствами имеют ряд преимуществ, то при создании подсистемы информационной защиты нового типа целесообразно прежде всего рассмотреть возможность применения аппаратных средств.

Укрупненная схема функционирования подсистемы защиты информации КС в зависимости от важности информации показана на рис. 3. При этом для определения коэффициента важности информации используются выражения (1) и (2), а для извлечения из соответствующей базы данных набора и параметров известных средств защиты поможет описание КС согласно (3). Для наполнения соответствующей базы данных имеется большое количество источников. Некоторый набор аппаратно-программных средств защиты информации в сетях и в локальном персональном компьютере приведен в [1– 6]. В таблице представлена лишь небольшая выборка такой информация для ЭВМ [1– 5].

ТАБЛИЦА. Средства информационной защиты ЭВМ

Наименование	Назначение	Производитель
1	2	3
eToken Enterprise	Защита электронного документооборота	Aladdin Software Security R.D.
Secret Disk	Защита конфиденциальной информации на персональном компьютере	Aladdin Software Security R.D.
SmartLogon	Программно-аппаратный комплекс защиты информации от НСД	SIS
S4Enterprise	Система разграничения доступа и шифрования	Мультисофт
СОБОЛЬ	Защита ресурсов компьютера от несанкционированного доступа.	НИП "Информзащита”
Аккорд-Рубеж-1.4	Программно-аппаратный комплекс для защиты рабочих станций	ОКБ САПР
Аккорд PC-104	Аппаратный модуль защиты	ОКБ САПР
Аккорд-АМД3	Аппаратный модуль для шины ISA, PCI и стандарта PC104	ОКБ САПР
Аккорд-СБ	Программируемый PCI-контроллер	ОКБ САПР
ViPNet SAFE DISK	Средство создания секретных дисков	Инфотекс
Crypton Lock	Модуль санкционированного доступа	Анкад
Secret Disk Professional	Криптографический модуль для съёмных носителей	Анкад

Окончание таблицы

1	2	3
Guardant	Электронный ключ защиты DOS Windows приложений	Технотрейд
Eutron Smart Key- Plus+	Электронный ключ защиты ПК	–
Система SHIELD	Программа контроля входа в ПК и разграничения доступа	–
Система DISK-REET	Программа защиты доступа к логическим дискам и данным	Пакет NORTON UTILITES

Несмотря на то, что вариантов средств защиты в конечном итоге – незначительное количество (часть их было отсечено ранее по параметрам показателя уровня защиты), все же решение задачи выбора оптимального набора аппаратных и программных средств защиты по выбранным критериям является сложной процедурой. Для её решения могут быть использованы, например, стоимостные модели, отображающие влияние затрат на степень защищенности системы [16, 17]. Сущность подхода заключается в построении и применении теоретико-игровой модели для анализа проектов защиты информации в КС и применении одношаговых конечных игр двух игроков – "защитника" и "нарушителя" [17]. На базе полученных результатов определяются предпочтительные проекты информационной защиты при условии, что эти проекты удовлетворяют и другим требованиям, в частности, по производительности КС, для оценки которой необходимо учитывать выражение (4).

Схема, показанная на рис. 3, может быть реализована специальным аппаратным модулем, который (как и другие модули расширения функциональных возможностей компьютерной системы) устанавливается в соответствующий слот расширения системной платы компьютера.

Сложность всей подсистемы защиты может быть существенно уменьшена (при том же уровне информационной защиты), если некоторые её функции перенести на устройство связи пользователя с компьютером.

Выводы. Таким образом, в работе предложены основные положения новой парадигмы построения подсистемы защиты, которая исходит из установления взаимосвязей между важностью информации и набором средств, необходимых для построения подсистемы защиты требуемого уровня. При этом учитываются архитектурно – структурная организация среды, в которой работает пользователь (отдельный компьютер, локальная или корпоративная сеть), а также критерии оптимизации (например, стоимость, производительность КС и др.). Приведенная авторами схема функционирования такой подсистемы защиты и результаты теоретических исследований позволяют сделать вывод о возможности динамической перестройки подсистемы на конкретный уровень защиты, исходя из степени важности циркулирующей в КС информации. Управление такой подсистемой можно возложить на аппаратный модуль расширения, который, как и

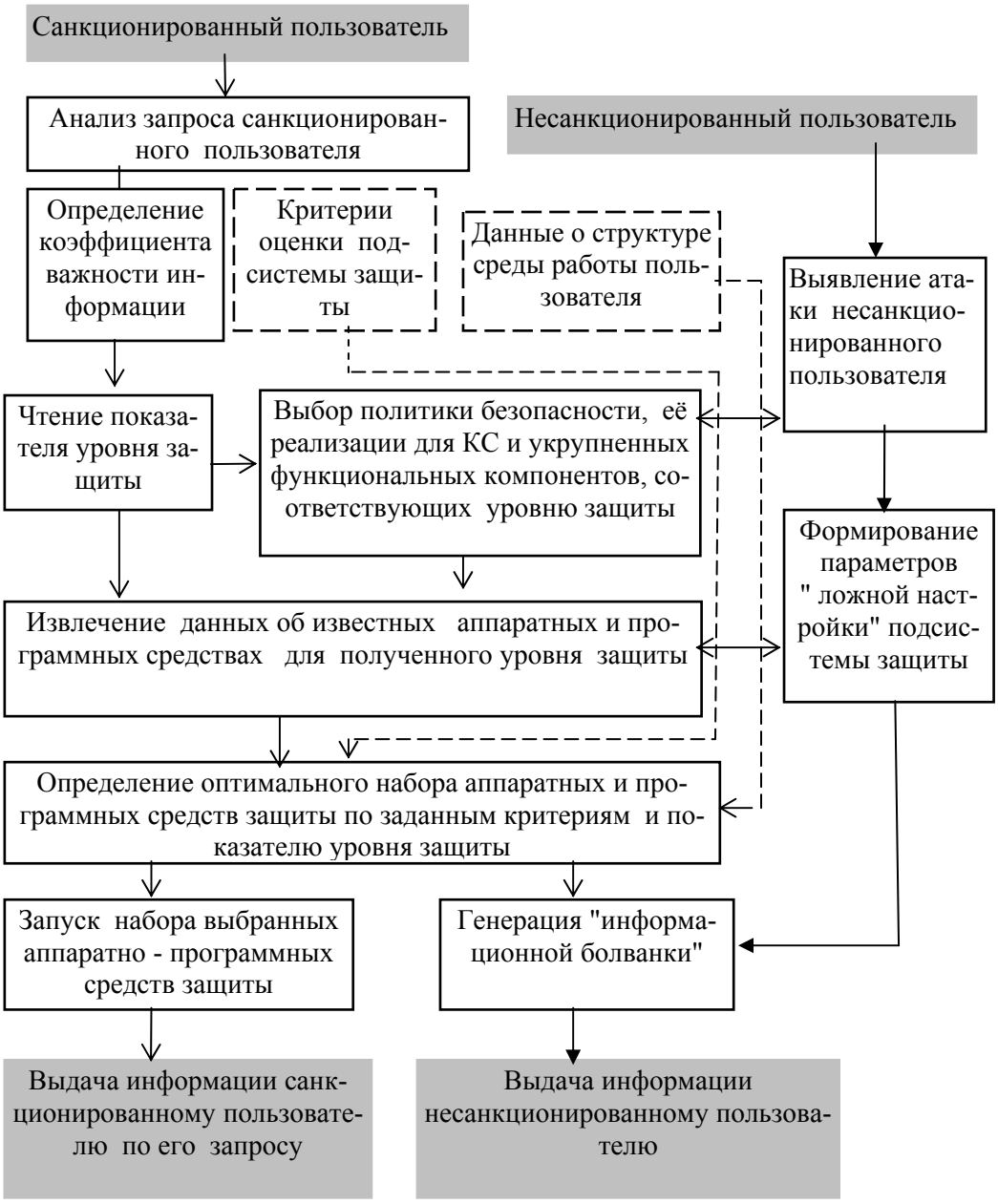

РИС. 3. Укрупненная схема функционирования подсистемы информационной защиты КС в зависимости от важности информации

другие модули, устанавливается в слот расширения материнской платы компьютера. При этом затраты на приобретение и использование средств защиты можно уменьшить (при том же уровне защиты), если часть функций информационной защиты (например, запуск системы, загрузка программ, защита диска от НСД и др.) реализовать аппаратно в составе оригинального устройства взаимодействия пользователя с компьютером.

Использование при построении средств информационной защиты предложенной парадигмы позволит существенно повысить производительность и эффективность КС при решении широкого класса задач, требующих различные уровни защиты информации.

1. *Дмитриев А*. Средства защиты информации // Мир ПК. – 2001. – №5.– С. 10– 26.
2. *Костюк Д*. Защита информации // Компьютеры + Программы. – 2002. – №3. – С. 12 –16.
3. *Астахов А*. Анализ защищенности корпоративных систем // Открытые системы. – 2002. – №7 – 8. – С.44 – 48.
4. *Средства* защиты информации от НСД. – http//www.pcmore.ru/security/naa/show.html.
5. *Комплексная* защита информации в персональных ЭВМ. – http//www.kiev-security.org.ua.
6. *Яковлев Ю.С. , Бардаченко В.Ф*. О проблеме безопасности информации в корпоративных сетях // Управляющие системы и машины. – 2003. – № 1. – С.71 –91.
7. *Русанівський В.М., Широков В. А.* Інформаційно – лінгвістичні основи сучасної тлумачної лексикографії // Мовознавство. – 2002. – №6. – С.7 – 48.
8. *Палагин А.В., Стерлигов В.А., Широков В.А.* Интенсификация научных исследований на базе высоких технологий // Труды междунар. науч. - практ. конф. KDS – 2001. – Т.1. – С. 516 –522.
9. *Киселев М., Соломатин Е.* Средства добычи знаний в бизнесе и финансах. Открытые системы. 1997. – №4. (http//www.osmag.ru).
10. *Семёнов И. А*. Представление знаний в объектно-ориентированной базе. – http://inftech.webservis.ru/it/database/oo/ar2.html
11. *Гринев М*. Системы управления полуструктурированными данными // Открытые системы. – 1999. – № 5-6. – С.45 – 53.
12. *Артемьев В.И*. Обзор способов и средств построения информационных приложений // Системы управления базами данных. – 1996. – № 5-6. – С.50-55.
13. *Дубова Н.* Устройство и назначение хранилищ данных // Открытые системы. – 1998. – № 4-5. – С.59 – 65.
14. *Гарбар П*. Организация отказоустойчивого хранилища // Открытые системы. – 2002. – №7-8. – С.56 – 61.
15. *Амстронг Р*. Семь этапов оптимизации производительности хранилища данных // Открытые системы. – 2002. – №1. – С.51 – 54.
16. *Нестеров С.А.* Об использовании конечных игровых моделей для оценки экономической эффективности систем защиты информации. – http://beda.stup.ac.ru/RV-conf/v01/014/index.html.
17. *Баутов А*. Экономический взгляд на проблемы информационной безопасности // Открытые системы. – 2002. – № 2. – С.34 – 37.

Получено 15. 06. 2003