INFORMATION SECURITY

УДК 004.056.53

СЕРГЕЙ ТОЛЮПА,
АЛЕКСАНДР УСПЕНСКИЙ

ПОСТРОЕНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ МНОГОУРОВНЕВОЙ ИЕРАРХИЧЕСКОЙ МОДЕЛИ

На современном этапе развития информационных технологий обеспечения информационной безопасности в масштабах всей информационной системы пока еще невозможно в силу отсутствия на рынке реальных решений, позволяющих строить именно интегрированные системы защиты информации. Поэтому в настоящее время оптимальным решением является построение именно комплексных систем защиты информации, построенных на основе многоуровневой иерархической модели. Одним из главных преимуществ представления систем защиты информации в виде иерархии функционально-независимых уровней является существенное упрощение процесса проектирования системы, поскольку проектирование одной многофункциональной и сложной системы можно разложить на несколько законченных этапов проектирования гораздо менее сложных систем для каждого уровня в отдельности, и завершающего этапа контроля целостности системы защиты при переходе от уровня к уроню.

Ключевые слова: защита информации, информационные технологии, безопасность, модель, целостность системы, средства защиты.

На современном этапе развития информационных технологий (ИТ), обеспечение информационной безопасности (ИБ) в масштабах всей информационной системы пока еще невозможно в силу отсутствия на рынке реальных решений, позволяющих строить именно интегрированные системы защиты информации (СЗИ). Это можно объяснить недостаточной зрелостью международных стандартов в области защиты информации, хотя движение в этом направлении прослеживается уже достаточно явно. С другой стороны, построение многокомпонентных, а тем более однокомпонентных СЗИ в большинстве случаев уже не является современным решением проблемы ИБ, особенно для крупных компаний. Поэтому в настоящее время оптимальным решением является построение именно комплексных СЗИ (КСЗИ), построенных на основе многоуровневой иерархической модели.

Как показывает практика, проектирование комплексной СЗИ является достаточно сложной системно-аналитической задачей, которая требует специальной и достаточно строгой методики.

Известно, что в области IT давно и достаточно успешно применяется стековая модель описания сложных ИС, в которой система рассматривается в виде иерархии нескольких функционально-единообразных уровней. Поскольку любая СЗИ в конечном итоге должна «накладываться» на реальную ИС, для ее описания также целесообразно было бы использовать многоуровневую иерархическую модель.

Одним из главных преимуществ представления СЗИ в виде иерархии функционально-независимых уровней является существенное упрощение процесса проектирования системы, поскольку теперь проектирование одной многофункциональной и сложной системы можно разложить на несколько законченных этапов проектирования гораздо менее сложных систем для каждого уровня в отдельности и завершающего этапа контроля целостности системы защиты при переходе от уровня к уроню [1].

Проблема обеспечения целостности системы защиты в рамках предложенной модели СЗИ принимает достаточно понятную и наглядную форму. Как уже было сказано, это

обеспечение полноты реализации функций защиты на каждом уровне модели СЗИ и обеспечение целостности функций защиты при переходе от уровня к уровню. Очевидно, что максимальная степень комплексности СЗИ достигается в том случае, когда применяемые технические средства, решения и методы обеспечивают защиту каждого уровня в соответствии с самыми жесткими требованиями и при этом все используемые с СЗИ технические средства проявляют свою функциональность на каждом уровне модели. Очевидно, что построить настолько "комплексную" СЗИ в принципе возможно только при неограниченных ресурсах проекта. Поэтому на практике необходимо найти разумный и, главное, обоснованный компромисс между "комплексностью" системы, т.е. ее функциональной наполненностью, и совокупной стоимостью ее построения и эксплуатации [2].

На наш взгляд, типовую СЗИ можно рассмотреть в виде следующих пяти функциональных уровней:

– физический уровень: физическая охрана помещений, в которых обрабатывается или хранится конфиденциальная информация; организация контроля доступа сотрудников в данные помещения; ответственное хранение резервных (архивных) копий конфиденциальных информационных ресурсов; обеспечение энерго- и пожаробезопасности всей ИС в целом и др.;

– технологический уровень: устранение угроз безопасности информации, связанных с использованием некачественных аппаратно-технических средств обработки и хранения информации и систем передачи данных; контроль качества (в т.ч. целостности) используемого программного обеспечения; организация резервных хранилищ данных, кластеров; периодическое архивирование данных; контроль лицензионной политики; организация защиты от вредоносных и разрушающих программ и т.д.;

– пользовательский уровень: устранение угроз, связанных с некорректными (случайными, ошибочными и т.д.) действиями персонала или умышленными действиями нелояльных сотрудников компании или третьих лиц (разграничение доступа к информационным ресурсам, защита от несанкционированного доступа (НСД), аутентификация пользователей, включая удаленных и мобильных сотрудников компании и т.д.);

– сетевой уровень: система защиты на этом уровне должна устранить угрозы, исходящие от злоумышленников, находящихся как внутри, так и вне пределов защищаемой ИС на уровне базовой сетевой инфраструктуры (сегментация локальных вычислительных сетей (ЛВС) по уровням конфиденциальности обрабатываемой информации, защита информации при ее передаче по внешним и внутренним каналам связи, защита от внешних вторжений и т.д.);

– уровень управления: организация связи с системой управления ИС; управление, координация и контроль осуществляемых организационных и технических мероприятий на всех низлежащих уровнях СЗИ; контроль полноты реализации функций защиты на каждом из уровней и неразрывности функционирования СЗИ при переходе от уровня к уровню; окончательный (а далее периодический) контроль стойкости и комплексности всей СЗИ в целом (например, путем применения специальных технических средств "дружественного взлома") и т.д.

Следует отметить, что в конкретной автоматизированной системе наличие всех пяти уровней СЗИ в явном виде не всегда обязательно, хотя стойкость системы защиты напрямую зависит от наличия каждого уровня и его функциональной наполненности. Очевидно также, что стоимость и сложность реализации СЗИ существенным образом растет от уровня к уровню, причем снизу-вверх. Так, например, значительную часть необходимых функций СЗИ на физическом уровне можно реализовать простыми и привычными организационными мерами, т.е. практически "бесплатно". А, например, на сетевом уровне для защиты сложных систем необходимо применение уже достаточно дорогостоящих технологий, таких как межсетевое экранирование, VPN, средства обнаружения вторжений и т.д. [3].

Следует отметить, что предлагаемый пятиуровневый "стековый" подход помимо упрощения самого процесса проектирования, позволяет четко формализовать три достаточно

сложные задачи, которые неизбежно возникают при создании систем защиты ИС:

– обеспечение целостности (комплексности) системы защиты;

– разграничение требований и функций СЗИ при защите информации, обладающей различной степенью конфиденциальности;

– обеспечение целостности СЗИ при защите территориально-распределенных ИС.

При этом при решении указанных задач в абсолютном большинстве случаев удается обеспечить оптимальное соотношение функциональность/стоимость СЗИ для владельца ИС и должным образом это обосновать.

Проблема обеспечения целостности системы защиты в рамках предложенной модели СЗИ принимает достаточно понятную и наглядную форму – это обеспечение полноты реализации функций защиты на каждом уровне модели СЗИ и обеспечение целостности функций защиты при переходе от уровня к уровню. Очевидно, что максимальная степень комплексности СЗИ достигается в том случае, когда применяемые технические средства, решения и методы обеспечивают защиту каждого уровня в соответствии с самыми жесткими требованиями и при этом все используемые в СЗИ технические средства проявляют свою функциональность на каждом уровне модели. Очевидно, что построить настолько “комплексную” СЗИ в принципе возможно только при неограниченных ресурсах проекта. Поэтому на практике необходимо найти разумный и, главное, обоснованный компромисс между “комплексностью” системы, т.е. ее функциональной наполненностью, и совокупной стоимостью ее построения, эксплуатации й восстановления [4]. Под стоимостью эксплуатации подразумевается уровень адаптируемости СЗИ (т.е. сохранение необходимого уровня защиты) к неизбежным изменениям состава и конфигурации ИС.

Практика показывает, что в настоящее время оптимальным подходом для обеспечения необходимой комплексности СЗИ является построение системы на базе таких продуктов, которые проявляют свои защитные функции на двух-трех, при этом не обязательно соседних, уровнях СЗИ (см. рис.1). И, очевидно, “проявляемые” на каждом уровне защитные функции должны полностью перекрывать налагаемые на защиту данного уровня требования. Сделать это возможно уже сегодня на основе имеющихся на рынке продуктов по защите информации. Так, например, существующие сегодня развитые продукты по реализации функций межсетевого экранирования, позволяют решать не только традиционные для межсетевых экранов задачи по фильтрации трафика на сетевом уровне, но и часть задач пользовательского уровня (аутентификация удаленных пользователей и задание политик безопасности для каждого пользователя при работе в открытой сети), технологического уровня (контроль входящего трафика на предмет наличия разрушающих и вредоносных программ) и уровня управления (целостное управление всем комплексом с единой консоли). Очевидно, что чем больше таких “многоуровневых” средств защиты применяется в СЗИ, тем легче ее проектирование и полнее и надежнее она выполняет свои функции.

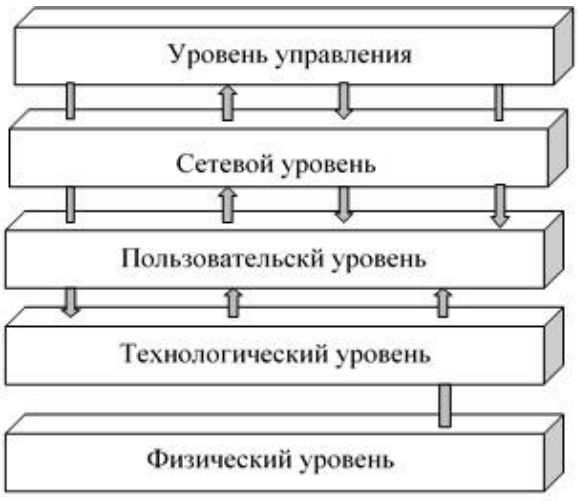

Рисунок 1 – Уровни защиты информации

Проблема разграничения системы защиты информации различной степени конфиденциальности заключается в том, что часто на практике в рамках одной ИС приходится “работать” с информацией, требования по защите которой существенно отличаются друг от друга. Так обрабатываемые и хранимые в рамках типовой ИС информационные ресурсы, как правило, разделяются на три группы: открытые информационные ресурсы, конфиденциальные информационные ресурсы, информационные ресурсы ограниченного доступа.

Очевидно, что защита всех разновидностей информационных ресурсов в рамках одной и той же СЗИ подразумевает, что даже открытые ресурсы будут защищаться по требованиям, предъявляемым к защите секретной информации. Очевидно, это приведет к необоснованно высокой стоимости СЗИ и большим неудобствам работы для персонала компании. Так же неэффективно будет построение трех различных СЗИ для каждого из ресурсов, поскольку, во-первых, четко разделить эти ресурсы в рамках одной ИС практически никогда не удается, а во-вторых, это опять приведет к повышению стоимости самой системы.

В рамках предложенной модели указанная проблема может быть решена путем разграничения требований и, соответственно, функциональности для каждого из уровней защиты СЗИ применительно к каждой группе информационных ресурсов. Сделать это тем более возможно, поскольку в пределах одного уровня требования к защите информации находятся “в одной системе координат”. При этом, если информационные ресурсы в каком-либо элементе ИС четко физически не разделены, в рамках СЗИ необходимо оценить возможность разделения указанных ресурсов на каждом из уровней системы. Если в пределах одного уровня сегментировать информацию не удается, система требований для данного уровня, очевидно, должна строиться исходя из требований по защите информации максимальной степени конфиденциальности. Если сегментация информации возможна, к уровню может предъявляться двойная (тройная и т.д.) система требований.

В подобных случаях необходимо применение несложных экономических расчетов по оценке эффективности того или другого решения.

Проблема обеспечения целостности защиты территориально-распределенных ИС заключается в том, что, как правило, даже большая корпорация не в состоянии обеспечить одинаковый уровень защиты для ИС Центрального офиса (ЦО) компании и всех ее филиалов (представительств, дочерних компаний и т.д.). На практике чаще всего ЦО защищается в соответствии с самыми жесткими требованиями по ИБ, а для системы защиты филиалов регламентируются только технические параметры взаимодействия с СЗИ ЦО. В большинстве случаев такой подход является вполне обоснованным, поскольку именно в ИС ЦО сосредоточены основные информационные ресурсы компании. Поэтому проблема, собственно, заключается в том, чтобы обеспечить целостность защиты СЗИ ЦО при ее информационном взаимодействии с СЗИ “менее защищенных” филиалов.

В рамках предложенного подхода сохранение целостности защиты корпоративной СЗИ обеспечивается в том случае, когда при взаимодействии двух систем СЗИ ЦО дополнительно контролирует те параметры защиты, которые не контролируются в СЗИ филиала. В случае же “прозрачного” взаимодействия двух систем на одном из уровней СЗИ (чаще всего пользовательском и сетевом) требования к данному уровню СЗИ филиала должны соответствовать аналогичным требованиям СЗИ ЦО.

Для успешного использования современных информационных технологий необходимо эффективно управлять не только сетью, но и системой защиты информации этой сети. Система, реализующая управление составом событий информационной безопасности должна работать автономно. Необходимо также разработать модель процесса планирования рационального модульного состава СЗИ каждого уровня, а также метод формирования рационального комплекса средств защиты на основе общих критериев [5].

В процессе организационно-технического управления, планирование ЗИ как функция управления представляет собой процесс последовательного снятия неопределенности относительно структуры и состава средств защиты в СЗИ. Процесс планирования ($P_{пл}$) рациональных наборов средств зашиты (СрЗ) характеризуется с помощью выражения

$$P_{\text{пл}} = \Phi \to S_r, \quad (1)$$

где Ф – множество функциональных подсистем для уровня защиты;

Sr – выбранный набор средств защиты.

На первом этапе задается множество функциональных подсистем для уровневой защиты, результатом планирования является командная информация, которая содержит конкретные данные по распределяемым ресурсам, направляемым на достижение целевого состояния СЗИ.

Процесс принятия решения о выборе рационального варианта набора СрЗ для каждого уровня защиты – это функция преобразования содержания информации о требованиях, предъявляемых к средствам защиты, входящим в набор, и характеристиках средств защиты, в подмножество наилучших вариантов набора $S' \subseteq S$. Множество вариантов набора

$$S = \{S_1, \ldots, S_r, \ldots, S_R\}, \quad (2)$$

где R – число вариантов альтернативных наборов, из которых осуществляется выбор.

Для выбора рационального варианта набора средств защиты используется целевая функция J:

$$S_r = J(S). \quad (3)$$

Совокупность сведений, позволяющих сопоставлять варианты наборов, это характеристики средств защиты функциональных подсистем для уровня безопасности – множество W, включающее в себя два подмножества:

$$W_{\text{зщ}_l} \subset W_l \text{ и } W_{\text{и}_l} \subset W_l, \quad (4)$$

где $W_{\text{зщ}_l}$ – показатель средств защиты “защищенность информации”;

W_{u_l} – показатель средств защиты “издержки” для *l-ой* функциональной подсистемы.

На основе морфологического подхода модель принятия решений (ПР) по выбору рационального варианта набора может быть представлена в виде кортежа:

$$ПР: \langle Ц, Ф, П_s, S, W_l, J, S_r(S') \rangle, \quad (5)$$

где $Ц$ – цель принятия решения;

$Ф$ – исходные данные для порождения вариантов набора средств защиты:

$\Phi = \{\Phi_1, \Phi_2, \ldots, \Phi_l, \ldots, \Phi_L\}$;

$П_s$ – правило порождения вариантов набора, которое может быть представлено в аналитическом виде как векторное произведение множеств

$$S = \Phi_1 \times \Phi_2 \times \ldots \times \Phi_l \times \ldots \times \Phi_L, \quad (6)$$

где Φ_l – множество, состоящее из средств защиты l-ой функциональной подсистемы

$$\Phi_l = \{A_{l1}, A_{l2}, \ldots A_{lm} \ldots, A_{lK_l}\}, \quad (7)$$

S – множество порожденных вариантов набора;

W_l – данные для выбора рациональных вариантов;

J – целевая функция для выбора рационального набора средств защиты (правило выбора);

S_r – рациональный набор средств защиты.

Отмечается, 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 [4].

В соответствии с трехуровневой моделью защиты, основой планирования рационального модульного состава СЗИ являются функциональные требования к наборам средств защиты (СрЗ) для каждого уровня, которые формулируются на основе нормативной документации, в соответствии с уровнем критичности обрабатываемой информации. Альтернативные средства защиты для каждой функциональной подсистемы набора средств защиты выбираются с учетом этих требований. Вариантов наборов, сертифицированных по

требуемому классу защищенности, может быть много. Сравнение вариантов наборов средств защиты предлагается производить по количественной мере.

Для решения задачи выбора рациональных вариантов наборов средств защиты для уровневой защиты разрабатывается метод обработки знаний, использующий неформализуемый опыт эксперта в области ЗИ, обеспечивающий преобразование сведений о характеристиках средств защиты из базы знаний и вывод решения в аналитической форме – метод формирования рационального комплекса средств защиты для СЗИ [5].

1. Разрабатываются варианты набора СрЗ. Множество возможных вариантов решения задачи выбора задается морфологической матрицей. Разрабатываются морфологические матрицы средств защиты для каждого уровня.

2. Заполняются вспомогательные матрицы, в которых отмечаются совместимые друг с другом программно-аппаратные средства. Вспомогательная квадратная матрица совместимых решений заполняется следующим образом: для каждой пары средств защиты разных функциональных подсистем определяется, совместимы ли они, и результат заносится в таблицу. Если СрЗ совместимы, то функция совместимости $s(A_{lm}, A_{pr}) = 1$, в противном случае $s(A_{lm}, A_{pr}) = 0$.

3. Генерируется множество решений по выбору вариантов набора СрЗ с усечением этого множества до подмножества вариантов набора из совместимых между собой программно-аппаратных продуктов.

Множество $S = \{S_1, \ldots S_r, \ldots, S_R\}$, состоящее из всех возможных вариантов построения набора СрЗ для уровня, является декартовым произведением множеств альтернатив.

Элемент множества

$$S_r = \left\{ \left(A_{1i}, A_{2j}, \ldots A_{lm}, \ldots A_{Ln} \right) : A_{lm} \in \Phi_l, \forall l = \overline{1,L} \right\},$$

где L – число функциональных подсистем для рубежа;

A_{lm} – средство защиты для реализации *l-ой* функциональной подсистемы.

Генерация множества решений по выбору вариантов набора, состоящих из совместимых между собой СрЗ, осуществляется следующим образом.

Происходит итерационный синтез вариантов набора, состоящих из совместимых СрЗ: на первом шаге перебираются последовательно варианты средств защиты для первой подсистемы, после выбора альтернативы A_{1i} осуществляется переход ко второму шагу. На втором шаге выполняется последовательный перебор вариантов средств защиты второй подсистемы, но выбор осуществляется только для таких альтернатив A_{2j}, для которых функция совместимости *s(* A_{1i} *,* A_{2j} *) = 1* и т.д. При выборе альтернатив из *l-ой* подсистемы выбор осуществляется только из таких альтернатив A_{lm}, для которых функции совместимости равны единице. Таким, образом, выбор СрЗ из каждой строки морфологической матрицы (по одной из каждой строки) для формирования варианта набора осуществляется только из совместимых между собой программно-аппаратных продуктов.

4. Дальнейшее усечение множества *S* выполняется методом полного перебора по заданной целевой функции. В качестве целевой функции для выбора варианта набора $S_r = \{A_{1i}, A_{2j}, \ldots A_{lm}, \ldots A_{Ln}\}$, применяется функция

$$J = \max_r \frac{W_{K_{\text{зщ}}}^{A_{1i}} + \ldots + W_{K_{\text{зщ}}}^{A_{lm}} + \ldots + W_{K_{\text{зщ}}}^{A_{Ln}}}{W_{K_{\text{и}}}^{A_{1i}} + \ldots + W_{K_{\text{и}}}^{A_{lm}} + \ldots + W_{K_{\text{и}}}^{A_{Ln}}}, \quad (8)$$

где $W_{K_{\text{зщ}}}^{A_{lm}}$ – значения показателя “защищенность”;

$W_{K_и^1}^{A_{lm}}$ – значения показателя «издержки» средства защиты A_{lm}.

Для оценки средств защиты разных функциональных подсистем наборов разрабатываются иерархические структуры обобщенных критериев качества средств защиты: показатель “защищенность” и показатель “издержки” [6].

Критерии качества средств защиты по иерархии “защищенность” делятся на две группы: показатели обеспечения эффективности оперативных методов защиты и показатели функциональной пригодности. Критерии качества по иерархии “издержки” делятся также на две группы: в первую включена стоимость соответствующего средства защиты, число пользователей по одной лицензии и другие возможные экономические издержки; ко второй группе издержек относятся функциональные издержки, такие, например, как падение производительности информационной системы при использовании данного средства защиты.

Оценка средств защиты и критериев осуществляется попарным сравнением по методу Т. Саати, результаты приводятся в числовом виде. С использованием иерархических структур критериев качества СрЗ вычисляются нормированные значения собственных векторов средств защиты по всем критериям до показателей “защищенность” $K_{\text{зщ}}^1$ и “издержки” $K_{\text{и}}^1$ на основании обработки всех матриц попарных сравнений с учетом связей критериев.

После выбора рациональных наборов средств защиты для рубежей защиты получен рациональный модульный состав целостного комплекса средств защиты объекта, удовлетворяющий требованию $J \rightarrow max$.

5. Оценивается, удовлетворяет ли сформированный комплекс средств защиты требованию

$$C\Sigma \leq Cдоп$$

где $C\Sigma$ – суммарные затраты на реализацию комплекса СрЗ;

$Cдоп$ – выделенные на реализацию комплекса денежные ресурсы.

Выбор комплекса средств защиты для СЗИ достигается итерационно путем приближения к рациональному составу, удовлетворяющему требованиям к допустимым затратам на его реализацию.

Структура системы интеллектуальной поддержки организационно-технического управления ЗИ, в которой реализуется метод формирования рационального комплекса средств защиты, представлена на рис. 2.

В системе интеллектуальной поддержки рациональные решения предлагается выбирать на основе использования экспертных знаний; в ней реализуется механизм приобретения знаний в процессе заполнения полей знаний экспертом при взаимодействии его с автоматизированной системой, выполняется совокупность процедур над проблемной областью с использованием многокритериального сравнительного анализа для выявления в заданном экспертом множестве подмножества наилучших по критериям предпочтения вариантов наборов, из которых формируется рациональный комплекс средств защиты.

Выводы. В рамках предложенной модели проблема безопасности может быть решена путем разграничения требований и, соответственно, функциональности для каждого из уровней защиты СЗИ применительно к каждой группе информационных ресурсов и средств защиты. Сделать это тем более возможно, поскольку в пределах одного уровня требования к защите информации находятся, можно сказать, “в одной системе координат”. При этом, если информационные ресурсы и средства защиты в каком-либо элементе ИС четко физически не разделены, в рамках СЗИ необходимо оценить возможность разделения указанных ресурсов на каждом из уровней системы. Если в пределах одного уровня сегментировать информацию не удается, система требований для данного уровня, очевидно, должна строиться исходя из требований по защите информации максимальной степени конфиденциальности.

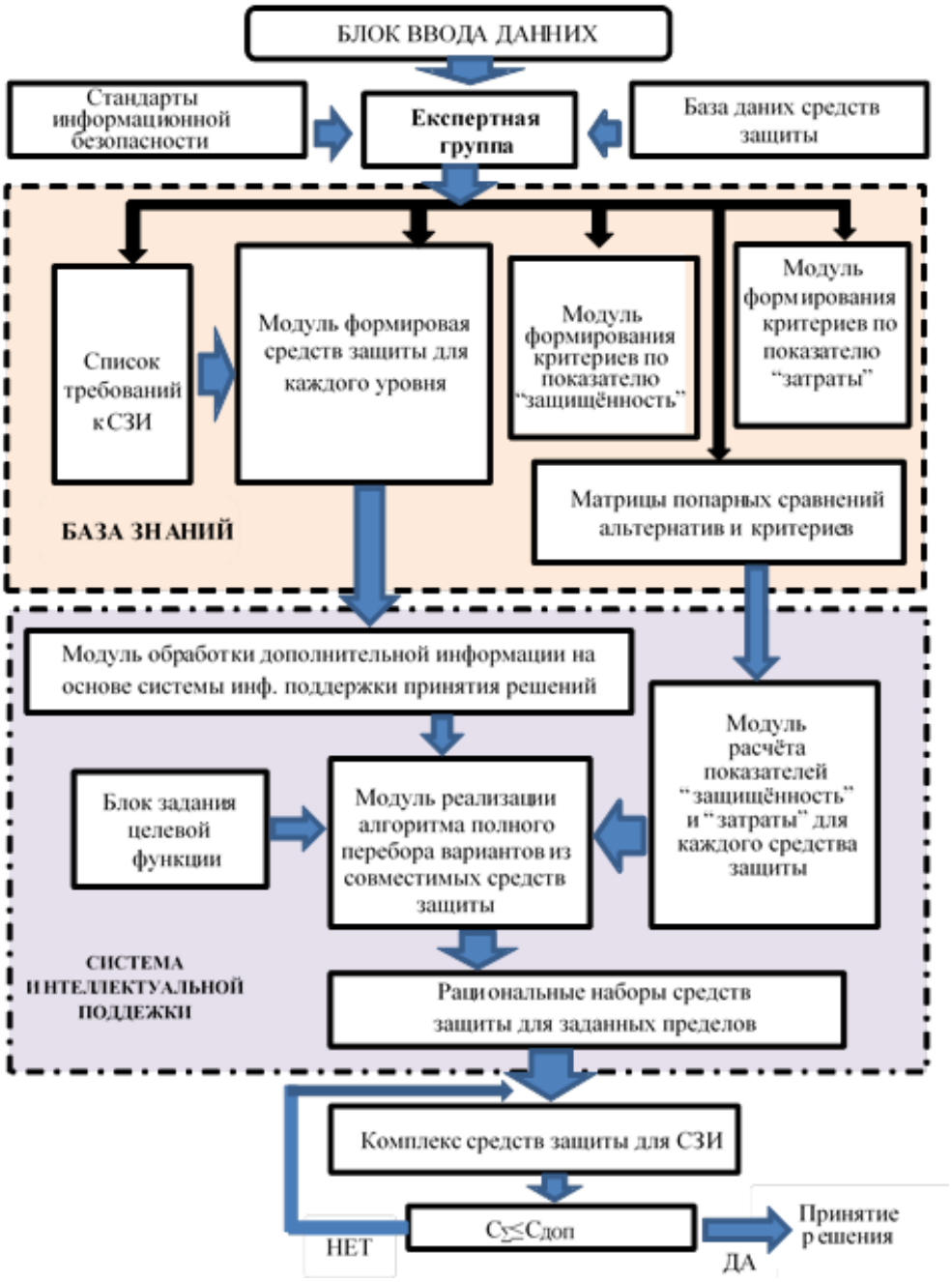

Рисунок 2 – Структура системы интеллектуальной поддержки организационно-технического управления ЗИ

В заключение еще раз подчеркнем, что предлагаемый подход к проектированию СЗИ на базе иерархии пятиуровневой модели носит достаточно общий (методический) характер и оставляет большое поле для творчества компаниям-проектировщикам. Предложенный системный подход позволяет существенно сократить сроки разработки СЗИ и при этом предложить заказчику действительно оптимальное и обоснованное решение.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] В.И. Андреев, Ю.Ю. Гончаренко, М.М. Дивизинюк, И.Н. Павлов, и В.А. Хорошко, *Проектирование систем технической защиты информации*. Севастополь, Украина: Изд. Центр СНУЯЭиП, с. 147-151, 2011.

[2] С.В. Толюпа, та І.І. Пархоменко, "Побудова комплексних систем захисту складних інформаційних систем на основі структурного підходу". *Сучасний захист інформації*, № 4, с. 96-104, 2015.

[3] И.Н. Павлов, “Проектирование систем защиты информации. Формальный подход”. *Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні,* вип. № 11, с. 54-59, 2005.
[4] С.В. Толюпа, “Проектирование систем поддержки принятия решений в процессе восстановления и обеспечения комплексной защити информационных системах”, *Сучасний захист інформації*, № 4, с. 69-74, 2012.
[5] С.В. Толюпа, В.С. Наконечный, и Ю.М. Якименко, ”Оценка защищённости информации в автоматизированных информационных системах с помощью общих критериев”, *Наукові записки Українського науково-дослідного інституту зв’язку*, № 6 (40), с. 27-31, 2015.
[6] С.В. Толюпа, В.С. Наконечный, и Ю.М. Якименко, “Обеспечение безопасности информации в автоматизированных информационных системах”, *Наукові записки Українського науково-дослідного інституту зв’язку*, № 5 (39), с. 33-37, 2015.

Статья поступила в редакцию 19.09.2016.

REFERENCE

[1] V.I. Andreev, Yu.Yu. Goncharenko, M.M. Divizinyuk, I.N. Pavlov, and V.A. Horoshko. *Technical security information system design*. Sevastopol, Ukraine: “SNUIAEiP” Publ, pp. 147-151, 2011.
[2] S.V. Tolyupa, and I.I. Parhomenko, “Organisation of integrated security information systems based on the structural approach”, *Modern ways of information securing,* no. 4, pp. 96-104, 2015.
[3] I.N. Pavlov, “Security information system design. Formal approach”, *Legal, standard and metrological secure software in Ukraine,* no. 11, pp. 54-59, 2005.
[4] S.V. Tolyupa, “Projecting of decision-making support systems in process of restoring and integrated securing of information systems”, *Modern ways of information securing*, no. 4, pp. 69-74, 2015.
[5] S.V. Tolyupa, V.S. Nakonechnyy, Yu.M. Yakimenko, “Information security evaluation in computer-controlled systems due to the general criteria”, *Scientific investigations of the Signals Research Study institute in Ukraine,* no. 6 (40), pp. 27-31, 2015.
[6] S.V. Tolyupa, V.S. Nakonechnyy, Yu.M. Yakimenko, “Information securing in computer-controlled information systems”, *Scientific investigations of the Signals Research Study institute in Ukraine,* no. 5 (39), pp. 33-37, 2015.

СЕРГІЙ ТОЛЮПА,
ОЛЕКСАНДР УСПЕНСЬКИЙ

ПОБУДОВА СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ БАГАТОРІВНЕВОЇ ІЄРАРХІЧНОЇ МОДЕЛІ

На сучасному етапі розвитку інформаційних технологій забезпечення інформаційної безпеки в масштабах всієї інформаційної системи поки ще неможливо в силу відсутності на ринку реальних рішень, які дозволяють будувати саме інтегровані системи захисту інформації. Тому, на наш погляд, в даний час оптимальним рішенням є побудова саме комплексних систем захисту інформації побудованих на основі багаторівневої ієрархічної моделі. Одною з головних переваг подання системи захисту інформації у вигляді ієрархії функціонально-незалежних рівнів є істотне спрощення процесу проектування системи, оскільки проектування однієї багатофункціональної і складної системи можна розкласти на кілька закінчених етапів проектування набагато менш складних систем для кожного рівня окремо і завершального етапу контролю цілісності системи захисту при переході від одного рівня до іншого.

Ключові слова: захист інформації, інформаційні технології, безпека, модель, цілісність системи, засоби захисту.

SERHII TOLIUPA,
OLEKSANDR USPENSKYI

BUILDING PROTECTION SYSTEMS ON THE BASIS OF INFORMATION MULTILEVEL HIERARCHICAL MODEL

At the modern stage of the development in the field of information technology it is still impossible to provide the software information security over the whole information system for lack of practical decisions in the market, which should work for organizing integrated information security systems in particular. So nowadays, in our opinion, the ultimate solution is to organize exactly these complex information security systems, developed on basis of hierarchical multilevel model. Obviously, it is generally possible to organize the integrated information security system, but only with limitless resources of the project. Therefore, a reasonable and, what is the most important, sufficient compromise between functional group of the system and aggregate value of its construction and exploitation is required to be found in practice. According to the suggested model, the security problem may be solved through delimitation of requirements and functionality for each of information security system levels naturally with reference to every group of the information resources and security tools. It is possible to put it into practice, because within the limits of one level requirements to information security are determined. One of the main advantages of presenting information security system as a hierarchy of functionally independent levels is significant simplification of system design, because the designing of one multifunctional and complex system may be divided into several finished stages of designing far less complicated systems for every level taken separately and for the finishing operation in order to control the security system integrity by stepping from one level to another. The suggested system approach enables to reduce time for information security system development and to offer a customer a really ultimate and reasonable decision at the same time.

Keywords: protection reporting purposes, information technology, security model, the integrity of system protection.

Сергей Васильевич Толюпа, доктор технических наук, профессор, профессор кафедры кибербезопасности и защиты информации, Факультет информационных технологий Киевского национального университета имени Тараса Шевченко, Киев, Украина.
E-mail: tolupa@i.ua.
Александр Анатольевич Успенский, кандидат технических наук, доцент, доцент кафедры кибербезопасности и применения автоматизированных информационных систем и технологий, Институт специальной связи и защиты информации Национального технического университета Украины “Киевский политехнический институт имени Игоря Сикорского”, Киев, Украина.
E-mail: uspensky@ukr.net.

Сергій Васильович Толюпа, доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації, Факультет інформаційних технологій Київського національного університету імені Тараса Шевченко, Київ, Україна.
Олександр Анатолійович Успенський, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та застосування автоматизованих інформаційних систем та технологій, Інститут спеціального зв’язку та захисту інформації Національного технічного університету України ”Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна.

Serhii Toliupa, doctor of technical sciences, professor, professor at the cybersecurity and information protection academic department, Faculty of information technology of Taras Shevchenko National university of Kyiv, Kyiv, Ukraine.
Oleksandr Uspenskyi, candidate of technical sciences, associate professor, associate professor at the cybersecurity and application of information systems and technologies academic department, Institute of special communication and information protection of National technical university of Ukraine “Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine.