УДК 004.056, 004.838.2

**О.В. Лукинова, А.В. Пугачев**

# Особенности построения профилей систем безопасности ИС

*Рассмотрены специфические вопросы построения функциональных и технологических профилей систем защиты, обеспечивающих безопасность информационных систем, в парадигме функциональной стандартизации; показано представление системы защиты на основе модели OSE/RM; исследованы состав и структура понятия «механизм защиты» с целью профилирования межкатегорийного представления системы защиты*

***Ключевые слова:*** *функциональная стандартизация, профиль, система защиты, механизм защиты.*

## PECULIARITIES OF CONSTRUCTION PROFILES OF SECURITY SYSTEMS OF INFORMATION SYSTEMS

*Examines the specific issues of building functional and technological profiles of the security systems to ensure the safety of information systems in the paradigm of functional standardization; shows a view of the system of protection based on the model of OSE/RM; studied the composition and structure of the concept of "defense mechanism" for the purpose of profiling third instalment correction representation of the system of protection*

***Keywords:*** *functional standardization, profile, protection system, protection mechanism.*

### Введение

Современные интегрированные информационно-телекоммуникационные системы представляют собой наиболее сложный класс информационных систем (ИС) с точки зрения методов и средств их проектирования, сопровождения и развития. К таким системам относятся корпоративные системы различного назначения и масштаба, электронные библиотеки и архивы, системы дистанционного образования и т.д. Их создание требует описания на уровне базовых стандартов и/или уникальных спецификаций объекта проектирования, причем, в силу сложности, эти описания должны применяться к отдельным частям объекта и интерфейсам между ними. Инструментом, позволяющим осуществлять подобные описания, является методология функциональной стандартизации (ФС), базирующейся на понятии профиля, под которым понимается «совокупность нескольких (или подмножество одного) базовых стандартов (и других нормативных документов) с четко определенными и гармонизированными подмножествами обязательных и факультативных возможностей, предназначенных для реализации заданной функции или группы функций» [1]. При этом, что касается ИС, то здесь выделяют функциональные профили, регламентирующие архитектуру и структуру системы и ее компонентов; и вспомогательные (технологические), которые описывают процессы жизненного цикла: формирование требований, концептуальное и детальное проектирование, эксплуатация, сопровождение и развитие ИС и ее компонент.

В [2] показано, что система безопасности, обеспечивающая защиту ИС согласно требований критериального вектора свойств конфиденциальности ($K$), целостности ($C$), доступности ($D$) и т.п. $\overline{KS}(C, D, K, ...)$, сформированного в результате анализа ценности бизнес-процессов предприятия, является неотъемлемой составной частью ИС. Статья посвящена исследованию специфических (в сравнении с технологией проектирования информационных систем) вопросов профилирования систем безопасности ИС.

### 1. Модель открытой среды как основа профилирования

Выше подчеркивалось, что ИС является сложным объектом, поэтому для успешного применения методологии ФС, ее необходимо представить в виде модели, которая позволяла бы в полной мере отразить функциональность ИС и декомпозировать ее на отдельные компоненты. Тогда появляется возможность профилирования и компонент системы, и интерфейсов между ними.

Свойства открытости, присущие данным системам, позволяют использовать для их представления модель открытой среды *OSE/RM (Open System Environment/Reference Model) IEEE POSIX* [3], которая синтезирует функциональность как ИС, так и системы защиты на референсном (эталонном, справочном) уровне.

Прежде всего модель представляет собой две части: прикладную

***Ольга Васильевна Лукинова,***
*к.т.н.*
*Тел.: (495) 334-89-70*
*Эл. почта: lobars@mail.ru*
*Институт проблем управления им. В.А.Трапезникова РАН (ИПУ РАН)*
*www.ipu.ru*

***Olga V. Lukinova,***
*candidate of technical Sciences, senior research associate,*
*Tel.: (495) 334-89-70*
*E-mail: lobars@mail.ru*
*The Institute of Control Sciences of the Russian Academy of Sciences (ICS RAS).*
*www.ipu.ru*

***Андрей Васильевич Пугачев,***
*аспирант*
*Тел.: +7(495) 434 -57-67*
*Эл. почта: mirea.os@ro.ru*
*Московский государственный технический университет радиоэлектроники и автоматики (МГТУ МИРЭА)*
*www.mirea.ru*

***Andrey V. Pugachev,***
*postgraduate*
*Tel.: +7(495) 434 -57-67*
*E-mail: mirea.os@ro.ru*
*Moscow State Technical University of Radio Electronics and Automation*
*www.mirea.ru*

и платформу, обеспечивающую функционирование приложений посредством системных сервисов, вызываемых с помощью API-функций (рис. 1). Она структурируется в виде матрицы компонент («клеток»), отражающих функциональные группы ИС, и содержит три уровня, и четыре группы функциональных компонент в каждом. Эти уровни следующие:

– компоненты служб и сервисов промежуточного слоя (*MW*);

– компоненты операционных систем или операционного слоя (*OW*);

– аппаратный слой (*HW*).

Функциональные группы компонент в данной модели составляют:

– компоненты, обеспечивающие интерфейс с пользователем (*User – «U»*);

– компоненты, обеспечивающие все необходимые в системе процессы (*System – «S»*);

– компоненты, обеспечивающие организацию, представление, доступ и хранение данных (*Information – «I»*);

– компоненты телекоммуникационной среды, обеспечивающие взаимосвязь информационных систем (*Communication – «C»*), данный уровень представляет собой известную модель взаимосвязи открытых систем (*OSI/RM – Open System Interconnection/Reference Model*).

Кроме того, модель трехмерна, она имеет несколько плоскостей: передняя (базовая) <ИС>, предназначена для структуризации основных функций, относящихся непосредственно к реализации прикладной (целевой) части ИС. Также имеются плоскость администрирования прикладной системы <А> и плоскость ее защиты <З>, которые отражают, каждая в своем контексте, функциональность базовой плоскости (кстати, стандарт [3] позволяет достраивать дополнительные плоскости под любые функциональные потребности).

Таким образом, понятие ИС включает и интегрирует в *единую систему* функциональность, по крайней мере, трех граней информационной технологии: прикладной (плоскость <ИС>), адми-

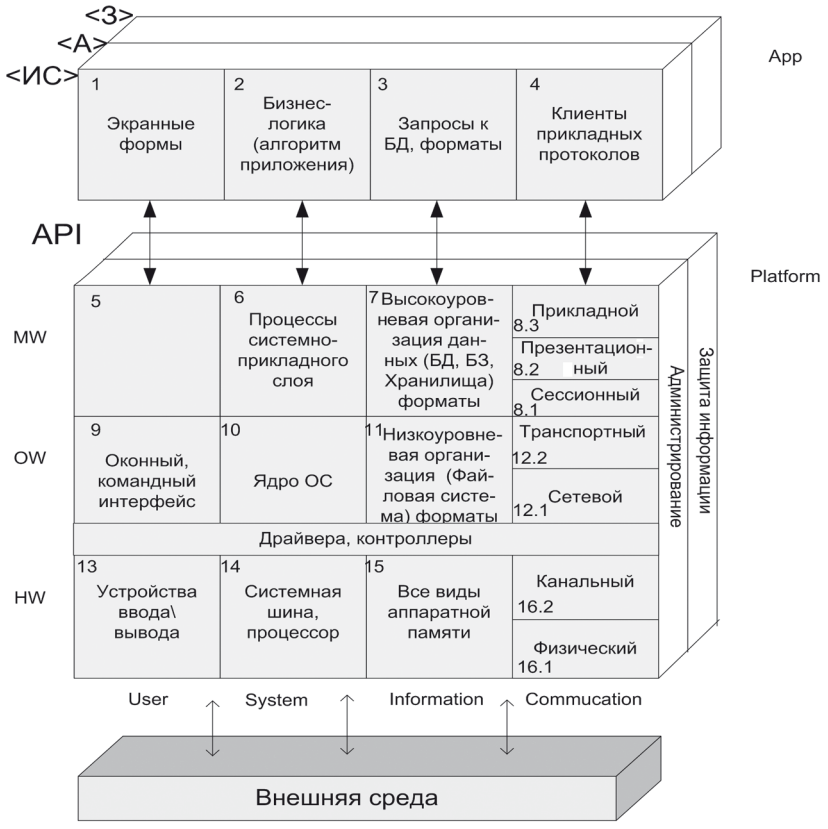


**Рис. 1.** Концептуальная модель OSE/RM.
Здесь <ИС> – плоскость функциональности ИС,
<А> – плоскость администрирования, <З> – плоскость защиты

нистративной (плоскость <А>) и защитной (плоскость <З>). Тогда возникает задача – формирование вектора требований безопасности для реализаций каждой «клетки» модели, т.е. формировании векторов $KS^{ИС}(C,D,K,...)$ для прикладной системы <ИС>, ее администрирования <А> – $KS^{A}(C,D,K,...)$ и защиты <З> – $KS^{З}(C,D,K,...)$ по каждой «клетке» соответствующей плоскости. Тогда получим плоскости требований по каждой из проектируемых систем. Особенность в том, что, если требования по плоскостям <ИС> и <А> определяются в результате декомпозиции вектора $KS(C,D,K,...)$ относительно всей ИС, который, как показано в [2], формируется на основе анализа бизнес-модели предприятия и модели угроз, то вектор требований к безопасности самой системы защиты («клеткам» плоскости <З>) $KS^{З}(C,D,K,...)$, может быть сформирован только после проектирования защиты <ИС> и <А>.

Представление плоскости защиты <З> возможно в 2-х аспектах:

1. «Клетки» плоскости <З> интегрируют совокупности механизмов, обеспечивающих защиту реализаций соответствующих «клеток» базовой плоскости <ИС>, администрирования <А> – межкатегорийный аспект <З`>. На рис. 2 это соответствие указано стрелками по «клеткам» верхнего слоя платформенной компоненты, хотя, разумеется, такие механизмы должны быть сопоставлены каждой «клетки» модели *OSE/RM*..Это означает, что, например, «клетка» 7 плоскости <З`> (<З.7>) аккумулирует все механизмы, обеспечивающие защиту «клеток» 7 плоскостей <ИС> и <А> в соответствии с критериальными векторами $KS^{ИС}(C,D,K,...)$, $KS^{A}(C,D,K,...)$ по данной «клетке» (нумерация «клеток» идет по рис. 1).

2. Система защиты прикладной ИС сама является информационной системой, поэтому ее функциональность в свою очередь тоже может быть структурирована в соответствии с базовым представлением <ИС> с поправкой на контекст (проектное представление <З``>).

Тогда *комплексной системой защиты (КСЗ)*, обеспечивающей безопасность прикладной системы, включая администрирование, назовем совокупность программно-технических средств защиты, реализующих механизмы межкатегорийной плоскости <З`>, построенную в соответствии с проектным представлением <З``>.

Для проектирования защиты самой КСЗ необходимо строить межкатегорийную плоскость <З```> относительно проектной <З``> согласно вектора требований $KS^{З}(C,D,K,...)$, затем проектную <З````> относительно <З```> и затем заниматься интеграцией проектных плоскостей <З``> и <З````>. В данной статье речь идет о вопросах профилирования только прикладной системы, т.е. плоскостей <З``> и <З``> относительно требований $KS^{A}(C,D,K,...)$ и $KS^{ИС}(C,D,K,...)$.

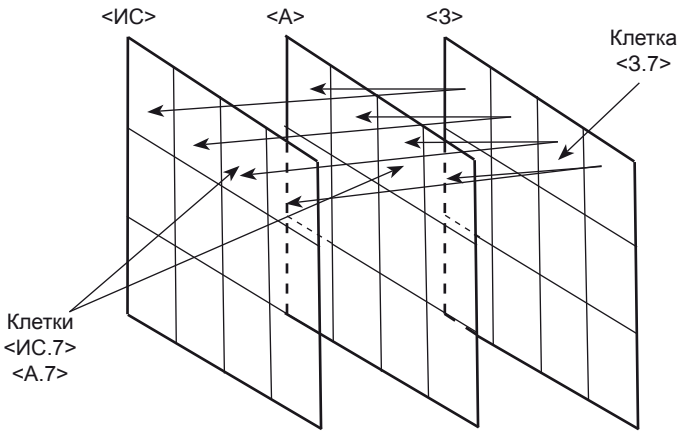


**Рис. 2.** Межкатегорийное соответствие механизмов защиты для плоскостей <ИС>,<А>

Таким образом, функциональный профиль КСЗ должен включать два документа: профиль межкатегорийного представления <З`> и профиль проектного представления <З``>. При этом, для профилирования плоскости <ИС> существуют и используются наработанные методы и технологии, основанные на представлении системы в виде модели *OSE/RM*. Результаты, описанные выше, позволяют применять те же подходы и к профилированию КСЗ, однако здесь имеется определенная специфика в части разработки как функционального, так и технологического профилей. Кроме того, требуется комплекс документов, не только профилирующих компоненты <З`> и <З``>, но и описания факторов и критериев для выбора того или иного технического решения.

## 2. Специфика построения функциональных профилей

**А) Особенности, связанные с межкатегорийным представлением <З`>**

А-1. Прежде всего, коль скоро межкатегорийная плоскость <З`> отражает совокупности механизмов защиты, сконцентрированных в «клетках» модели *OSE/RM*, следует пояснить, что представляет собой понятие «механизм защиты» [4].

Под *механизмом защиты* (*Мх*) будем понимать способ обеспечения требований безопасности без указания конкретной реализации, который может быть представлен теми или иными методами. В качестве *Мх* рассматриваются: механизмы управления доступом, контроля целостности, идентификации и аутентификации и др.

*Метод защиты* (*М*) также может быть реализован несколькими способами (например, идентификацию субъекта можно осуществить разными методами: паролем, методом биометрических характеристик, электронной карточкой). Реализация метода может быть выполнена одним или несколькими различными *алгоритмами* (*А*).

Таким образом, понятие *Мх* представляется иерархией рефе-

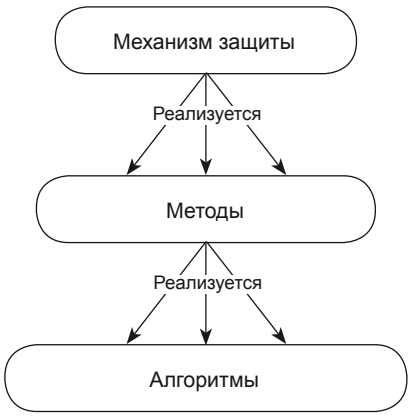


**Рис. 3.** Уровни представления понятия «механизм защиты»

ренсности $Mx(M(A))$ (рис. 3), т.е. каждый *Mx* может быть реализован тем или иным методом, а каждый метод – тем или иным алгоритмом. Например, управление доступом, т.е. авторизованный доступ к объектам ИС на требуемом уровне и в соответствующем режиме, можно осуществлять мандатным или дискреционным методом, или иным. Нижний уровень – алгоритмический, тот же дискреционный метод может быть реализован атрибутными схемами, списками полномочий и т.п.

Выбор конкретной цепочки $Mx(M(A))$ зависит от:

а) Требуемого уровня безопасности, задаваемого вектором значений $\overline{KS^{ИС}}(C,D,K,...)$ или $\overline{KS^{A}}(C,D,K,...)$ для соответствующей «клетки» плоскости.

б) Требований нормативных регуляторов для государственных систем (например, согласно методическому документу «Меры защиты информации в государственных информационных системах», утвержденному федеральной службой по техническому и экспортному контролю (ФСТЭК) 11 февраля 2014 г., следует применять меры защиты, основанные на *Mx* идентификации и аутентификации субъектов и объектов доступа к СУБД государственного назначения).

в) Дополнительно для алгоритмов выбор определяется параметрами эффективности (затратами памяти, временем на выборку значений, удобством ведения данных о субъектах и объектах доступа, удобством отслеживания ограничений и зависимостей по наследованию полномочий и др.), а для криптоалгоритмов – оценками стойкости. При этом для получения более достоверных оценок стойкости необходимо использовать алгоритмы, основанные на государственных или международных стандартах, например, ГОСТ 34.10-2012, описывающий криптопреобразование усиленной электронной подписи, а также параметры эллиптических кривых для генерации ключа электронной подписи. А с учетом сертификационных требований российским предприятиям целесообразно использовать российские ГОСТы и нормативно-рекомендательные документы при построении профилей систем безопасности корпоративных ИС.

Поэтому в профиль целесообразно включать: а) ГОСТы или иные нормативные документы, описывающие выбранный алгоритм, т.к., особенно для криптоалгоритмов, именно стандарт позволяет реализовать алгоритм с более достоверной оценкой стойкости, что позволит обеспечить защитные свойства механизмов в соответствии с уровнем критериев $\overline{KS}(C,D,K,...)$ или требованиями регуляторов; б) спецификации, отражающие те критерии и требования, на основе которых происходил выбор метода или механизма.

Таким образом, межкатегорийный профиль должен на уровне ГОСТов, нормативных документов и спецификаций фиксировать проектное решение цепочки «механизм-метод-алгоритм» $Mx(M(A))$ для каждой «клетки» <ИС> и <А> в соответствии с критериями а) – в).

А-2. Следующая особенность связана с семантической неоднородностью механизмов защиты, что позволило структурировать *Mx* на три категории, и их взаимосвязью.

**Группа 1.** Основные или целевые $Mx(Ц)$: обеспечивающие свойства безопасности $\overline{KS}(C,D,K,...)$, реализаций «клеток» всех трех плоскостей: <ИС>, <А>, <З>.

**Группа 2.** Обеспечивающие $Mx(O)$, те, которые осуществляют дополнительные действия, необходимые для функционирования целевых *Mx* на том или ином уровне безопасности. Например, идентификация и аутентификация (в некоторых случаях по требованию заказчика этот *Mx* может входить в группу основных механизмов); организация сеанса с ИС; организация доверенного канала/маршрута (туннелирование); защита (уничтожение) остаточных данных; защита периметра от внешних воздействий с помощью межсетевых экранов и т.д.

Целью обеспечивающих *Mx* является удовлетворение потребностей целевых, т.е. эти *Mx* осуществляют дополнительные действия, необходимые для: а) организации функционирования целевых *Mx*, б) осуществления целевым *Mx* своего назначения на том или ином уровне.

Например, если к объекту БД («клетка» <ИС>.7 рис. 1), для которого установлены те или иные права доступа (определен критерий конфиденциальности К), обращается некий субъект, то необходимо использовать механизм управления доступом (соответствующую цепочку $Mx(M(A))$) и описать в профиле, помимо цепочки $Mx(M(A))$, следующие механизмы из группы обеспечивающих:

1. механизм организации сеанса с ИС, чтобы предоставить возможность пользователю обратиться к СУБД;

2. механизм аутентификации субъекта (пользователя), который хочет обратиться к объекту СУБД, чтобы понять, что данный субъект является тем, кем он идентифицировался;

3. механизм идентификации и аутентификации объекта СУДБ;

4. механизм управления доступом (цепочка $Mx(M(A))$), который сопоставит права пользователя (субъекта) и файла (объекта), чтобы убедиться, что субъект обладает соответствующим правом.

5. чтобы обеспечить конфиденциальность файла на определенном уровне, надо использовать алгоритмы шифрования соответствующей стойкости механизма криптоподдержки.

Таким образом, каждый *Mx* из группы 1 требует поддержки обеспечивающих $Mx(Ц) \rightarrow (Mx(O_1), Mx(O_2), \ldots, Mx(O_n))$. Поэтому на самом деле межкатегорийная плоскость включает не только *Mx*, обес-

печивающие $\overline{KS}(C, D, K, ...)$, т.е. целевые, но к каждому целевому выстраивается и набор обеспечивающих $Mx(Ц) \rightarrow (Mx(O_1), Mx(O_2), \ldots, Mx(O_n))$, которые также подлежат профилированию по методике пункта А-1.

**Группа 3.** Управляющие механизмы *Mx*(*У*), те, которые обеспечивают согласованное функционирование *Mx* 1-й и 2-й групп. Это – мониторинг и аудит событий, происходящих в системе; анализ защищенности, т.е. выявление и анализ уязвимостей прикладной и платформенной компонент *OSE/RM*; оценка рисков, сопровождающих функционирование системы; администрирование системы безопасности.

**Б) Особенности, связанные с проектным представлением <З``>**

При профилировании проектного представления <З``> возникают две задачи.

а) Собственно формирование проектного представления <З``>, т.е. понять, в виде какой компоненты модели *OSE/RM* необходимо реализовывать *Mx* межкатегорийного представления. Понятно, что, например, управляющие механизмы реализуются как отдельные приложения. Решение этого вопроса для целевых и обеспечивающих *Mx* зависит от:

– влияния расположения механизма в системе на вклад в защиту «клеток» одного уровня и расположенных выше «клетки» локализации (чем ниже встроен *Mx*, тем большему количеству «клеток», расположенных выше по модели он обеспечит защиту);

– влияния локализации *Mx* на производительность других компонент системы.

б) Профилирование компонент сформированного проектного представления <З``>, а также межкомпонентных интерфейсов в соответствии со стандартами и спецификациями, связанными с системотехнической структурой КСЗ как информационной системы.

Имеется в виду, что комплект документов на проектирование КСЗ должен содержать:

а) Профили приложений, реализующих защитные механизмы межкатегорийной плоскости. Объектами стандартизации профиля приложений являются компоненты приложений в структуризации *USIC* (см. рис. 1), а также программные интерфейсы между компонентами и приложениями;

б) Профили среды, которые определяют сервисы, предоставляемые приложениям со стороны платформенной компоненты (промежуточный слой); услуги операционных систем, а также требования и интерфейсы к устройствам аппаратного слоя (рис. 4).

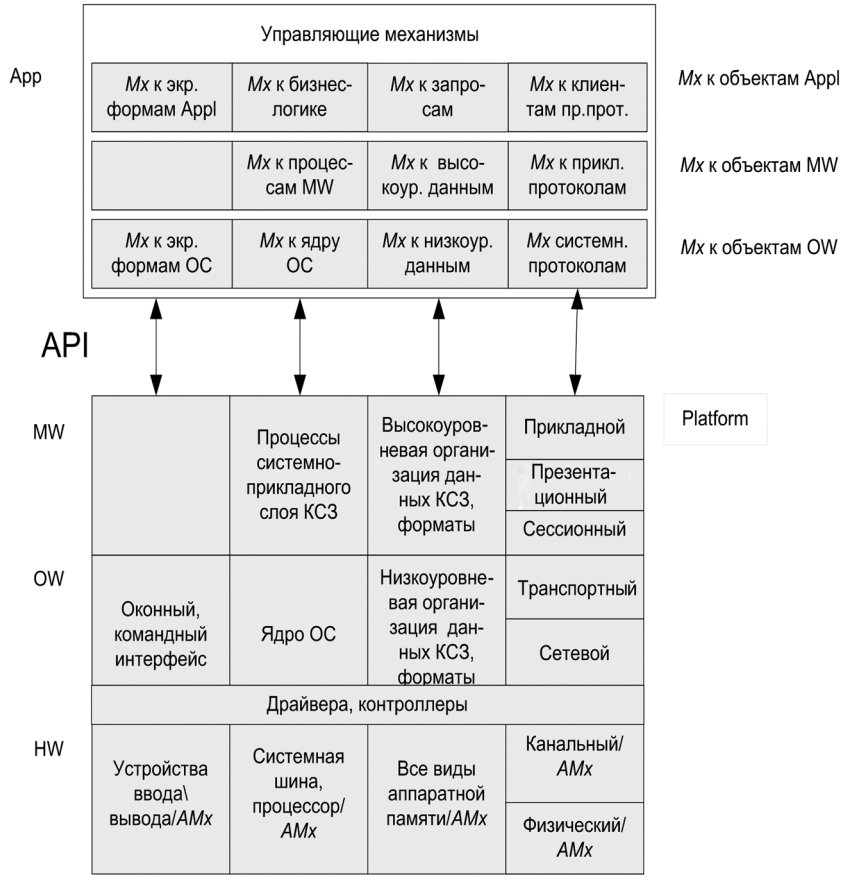


**Рис. 4.** Пример проектного представления плоскости <З``>

## 3. Особенности построения технологических профилей

Технологический профиль, как указывалось выше, определяется совокупностью нормативных и методических материалов, регламентирующих набор процессов (этапов) жизненного цикла (ЖЦ) конкретной ИС и ее компонент, содержание и применение этих процессов в соответствии с той или иной моделью ЖЦ. Целесообразность построения технологического профиля определяется необходимостью управления ЖЦ столь сложного объекта, как ИС, которая включает систему защиты в виде дополнительных плоскостей модели *OSE/RM*. Представление целевой ИС и системы ее защиты в виде единого интегрированного объекта позволяет совместить ЖЦ обеих систем. На рис. 5 показана детальная схема совмещения ЖЦ, которая хорошо демонстрирует, что

– методологически ЖЦ обеих систем одинаковы и включают однотипные работы: формирование требований как для ИС, так и требований безопасности в виде обеспечения свойств конфиденциальности, целостности, доступности и т.п. для КСЗ; концептуальное проектирование в виде разработки функциональной архитектуры для ИС и межкатегорийной плоскости механизмов <З`> для КСЗ; разработка системо-технической структуры ИС и аналогичной проектной плоскости <З``> с последующей интеграцией программно-аппаратных реализаций защитных механизмов для КСЗ; реинжиниринг бизнес-модели и, соответственно,

модификация ИС и перепроектирование КСЗ по результатам анализа осуществления ею защитных мероприятий, изменений бизнес-условий или требований безопасности, включая нормативные изменения, на стадии сопровождения.

– отправной точкой для разработки требований к обеим системам является наличие бизнес-модели, т.е. совокупности бизнес-процессов предприятия, подлежащих реализации целевой ИС. Особенностью этапа консалтинга для КСЗ является проработка компонент модели угроз на референсном уровне и оценка ценности бизнес-процессов с точки зрения их вклада в результаты предприятия с тем, чтобы на этой основе (и с учетом модели угроз) выставить требования безопасности в виде векторов $\underline{KS}(C, D, K, ...)$ к функционированию бизнес-процессов, а затем декомпозировать их на требования, предъявляемые к отдельным «клеткам» реализаций модели *OSE/RM* (межкатегорийная плоскость требований *TP*). Эти особенности должны быть отражены в спецификациях, отражающих указанные работы и алгоритмы;

– стадия проектирования характеризуется формированием межкатегорийной и проектной плоскостей КСЗ, принципы построения которых описаны выше; уточнением модели угроз в части уязвимостей, что может повлечь изменение перечня предполагаемых атак; кроме того, *Mx* могут быть реализованы как в виде отдельных приложений (наложенные средства защиты), составляющих прикладную часть проектного представления КСЗ, так и являться частью покупного программного средства, включаемого в состав ИС, т.е. быть встроенными. Это означает, что «клетка» межкатегорийной плоскости <З`> включает как наложенные, так и встроенные *Mx*. Поэтому, вообще говоря, возникает потребность в оценке вклада уровня безопасности, получаемого от встроенных *Mx* и от наложенных. Поэтому на этой стадии также возникает потребность в дополнительных спецификациях, вносимых в профиль;

– вводиться в эксплуатацию обе системы могут и должны одновременно как единый объект, назначение которого в том, чтобы: а) решать бизнес-задачи предприятия посредством прикладных приложений плоскости <ИС>, б) осуществлять администрирование платформенных компонент (плоскость <А>), в) осуществлять защиту объекта (плоскость <З>) от информационных угроз. Поэтому на временных диаграммах Ганта процессы, сопровождающие разработку систем, должны быть построены с учетом единой временной точки.

– стадия сопровождения включает анализ факторов, изменение которых повлечет необходимость модификации КСЗ. Эти факторы следующие: условия ведения бизнеса или целевые установки руководителя, требования нормативных документов безопасности, модель угроз.

Таким образом, описанная специфика означает:

а) Помимо унифицированных процессов, описываемых рядом отечественных и зарубежных стандартов [5–7], ЖЦ КСЗ предполагает выполнение ряда уникальных, свойственных только системе защиты, видов деятельности. Очевидно, что способы выполнения этих работ, критерий принятия тех или иных решений при их выполнении, должны быть включены в профиль, хотя бы на уровне спецификаций;

б) Стратегия построения профиля ЖЦ КСЗ, как и прикладной ИС, должна основываться на гибком сочетании отечественного ГОСТа 34.601, который позволяет осуществлять лучшую структуризацию ЖЦ с точки зрения планирования работ по реализации проекта, стандартов [5–7], описывающих полный набор процессов ЖЦ системы и спецификаций, касающихся особенностей КСЗ и дополняющих стандартный набор процессов.

## Заключение

В работе показано, что, имея полный профиль на систему, включающий функциональные и технологические профили, как на реализацию основных функций ИС, так и систему ее защиты, можно обеспечить методологическую основу для разработки и внедрения ИС и КСЗ как единого объекта. Однако, приведенные особенности функционального профиля системы безопасности, а также вопросы формирования технического профиля, демонстрируют нетривиальность задачи качественного построения этих документов. По этим причинам разработка методических рекомендаций, связанных с проектированием и поддержкой в рабочем состоянии функциональных и технологических профилей ИС на всех этапах ЖЦ и учитывающих описанные особенности, является актуальной задачей и требует дополнительных исследований.

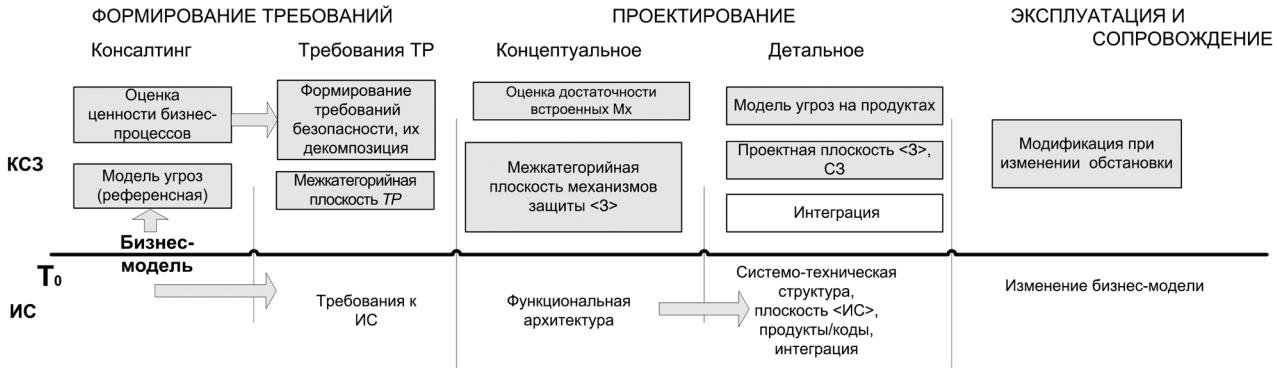


**Рис. 5.** Схема совмещения жизненного цикла ИС и КСЗ

**Литература**

1. ГОСТ Р ИСО МЭК ТО 10000-1-99 Информационная технология. Основы и таксономия международных функциональных стандартов. Часть 1. Общие положения и основы документирования. 1999.
2. *Лукинова О.В*. Методологические предпосылки к совмещению жизненных циклов информационной системы и системы ее защиты // Информационное общество. 2013. – № 5 . – С. 44–55.
3. IEEE Std 1003.0-1005, IEEE Guide to the POSIX Open System Enviroment (OSE) – N-Y.: The Institute of Electrical and Electronics Engineers, 1995. – 194 p.
4. *Лукинова О.В*. Семантическое описание факторов безопасности информациионных систем при проектировании систем защиты // Системы высокой доступности. 2013. – № 3 . – С. 149–156.
5. ГОСТ Р ИСО/МЭК 12207-11 Информационная технология. Процессы жизненного цикла программных средств. Стандартинформ. 2011.
6. ГОСТ 34.601.90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. Госстандарт СССР. 1990.
7. ГОСТ Р ИСО/МЭК 15288-05. Информационная технология. Процессы жизненного цикла систем. Стандартинформ. 2006.

**References**

1. GOST R ISO IEC THE 10000-1-99 Information technology. Framework and taxonomy of international functional standards. Part 1. General provisions and basic documentation.1999.
2. *Lukinova O. V.* Methodological background to the overlapping life cycles of information systems and its protection system // Information society. 2013. – No. 5. – P. 44–55.
3. IEEE Std 1003.0-1005, IEEE Guide to the POSIX Open System Environment (OSE) – N-Y.: The Institute of Electrical and Electronics Engineers, 1995. – 194 p.
4. *LukinovaO. V.* The semantic description of the safety factors of information extraction systems in the design of protection systems // high availability Systems. 2013. – No. 3 . – P. 149–156.
5. GOST R ISO/IEC 12207-11 Information technology. Processes software life cycle. STANDARTINFORM. 2011.
6. GOST 34.601.90. Information technology. A set of standards for automated systems. The automated control system. The stage of creation. Gosstandart of the USSR. 1990.
7. GOST R ISO/IEC 15288-05. Information technology. The life cycle processes systems. STANDARTINFORM. 2006.