Лукинова О.В.

МЕТОД КОНСТРУИРОВАНИЯ БИЗНЕС-ПРОЦЕССОВ, ОБЕСПЕЧИВАЮЩИХ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ, НА ОСНОВЕ МЕЖКАТЕГОРИЙНОГО ПРЕДСТАВЛЕНИЯ ПЛОСКОСТЕЙ ЗАЩИТЫ МОДЕЛЕЙ *OSE\RM*

Описана процедура построения бизнес-процессов обеспечения безопасности ресурсов информационной системы, которая является средой функционирования автоматизированных бизнес-процессов предприятия и представляется в виде референсной модели открытой среды.

***Ключевые слова**: комплексная система защиты, информационная система, модель OSE\RM, бизнес-процесс, механизм защиты.*

Введение

Сегодня разработка любой серьезной информационной системы предполагает использование определенной технологии, начальный этап которой заключается в том, что моделируются бизнес-процессы предприятия или некоторой области деятельности [1], подлежащие автоматизации. Совокупность таких бизнес-процессов фактически представляет модель деятельности предприятия, которая в дальнейшем реализуется в виде информационной системы. Такая методология позволяет:

1. Осознать и выстроить иерархию целей, которым должна удовлетворять будущая система;
2. Сформировать набор требований к системе, достаточный для реализации нужного функционала системы;
3. «Поиграть» имитационной моделью будущих бизнес-процессов с целью их оптимизации или лучшего структурирования. Для этого на сегодняшний день существует ряд инструментов, таких как BPEL, CaseWeise и др.

Аналогичный подход авторы применили к процессу проектирования комплексной системы защиты (КСЗ) для ИС, т.е. задача заключалась в том, чтобы

a) сконструировать бизнес-процессы, обеспечивающие безопасность информационной системы и реализуемые в виде приложений КСЗ;

b) найти способ их формализовать.

Постановка задачи обеспечения безопасности ИС

Постановка задачи обеспечения безопасности ИС, которая является реализацией совокупности бизнес-процессов предприятия, должна включать, по мнению авторов, следующие факторы (рис.1):

1. ИС, как объект защиты с одной стороны и как информационная бизнес-модель предприятия с другой. При этом значимость для бизнеса информационных потоков, обрабатываемых функциями бизнес-процесса предприятия или самих функций определяет и уровень защиты, и ущерб, наносимый бизнесу при ее нарушении.

2. Целевая функция для КСЗ должна быть сформулирована, как обеспечение основных свойств безопасности к информационным и вычислительным ресурсам ИС (ОЗ), а именно: *конфиденциальность (К)* – понимается как ограничение доступа к ресурсам в процессе хранения, обработки или передачи, *целостность (С)* – определяется неизменностью ресурса в процессе передачи или хранения (возможность модификации только уполномоченными лицами), *доступность (D)* – возможность получения легитимным пользователям некоторой услуги в заданный период времени. Иногда в это подмножество входит требование неотказуемости действий, происходящих в системе. Для оценки целевой функции вводятся одноименные критерии, такие как вектор безопасности $\overline{KS}(C,D,K)$, или $\{\overline{KS}\}=\{C,D,K,N\}$, где N – требование неотказуемости действий, измерение которых производится с помощью лингвистических или балльных шкал. Эти шкалы позволяют измерять и задавать уровень требуемой безопасности, а значения уровня определяются значимостью элементов бизнес-процесса предприятия.

3. Внешними воздействиями, которые могут нарушить целевую функцию, являются потенциально-опасные угрозы. Такая угроза характеризуется вероятностью возникновения, которая определяется наличием нарушителя и вероятностью реализации уязвимости программно-аппаратного обеспечения.

4. Защитные механизмы (*Mx*) представляют собой управляющие параметры, обеспечивающие заданный уровень целевой функции $\overline{KS}(C,D,K)$.

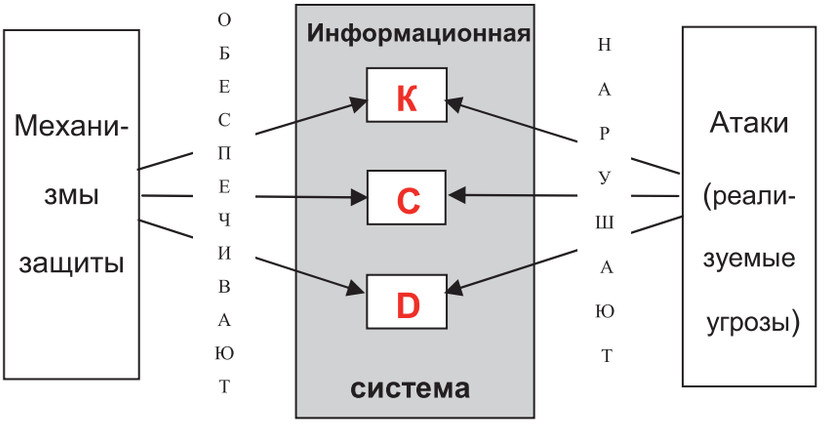

Рис. 1. Схема постановки задачи обеспечения безопасности ИС

Далее возникает задача представить ИС, как объект защиты в виде некоторой модели, причем модель должна в полной мере отражать функциональность ИС и позволять декомпозировать основные цели по функциональным группам ОЗ.

Для представления ИС была использована референсная модель среды открытых систем OSE/RM (Open System Environment/Reference Model), которая описывает эталонную функциональность

архитектуры и структуры информационной системы. Эта модель разработана группой POSIX и описана в стандарте [2,3].

Модель представляет собой два компонента: приложения, которые, собственно и реализуют функции, как бизнес-процесса предприятия, так и бизнес-процесса защиты, и платформу, обеспечивающую функционирование приложений посредством системных сервисов, вызываемых с помощью API-функций.

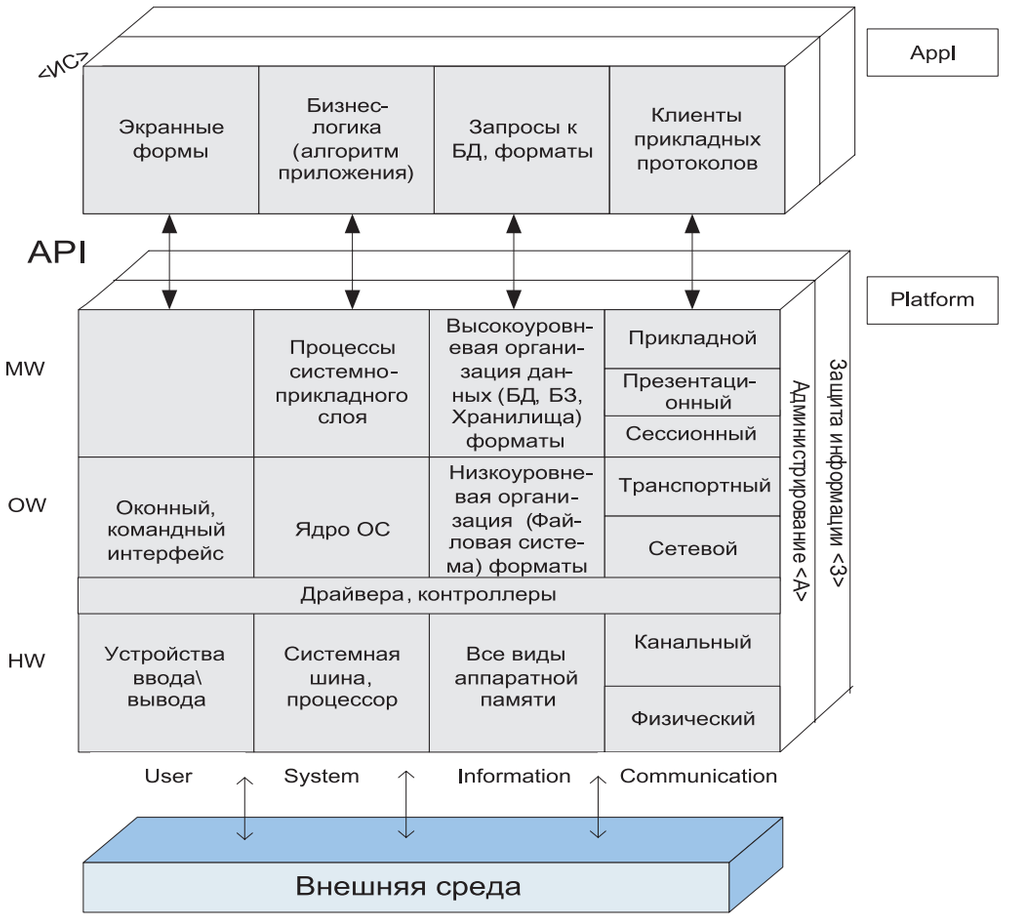

Рис. 2. Модель OSE\RM

Передняя базовая плоскость <ИС> предназначена для структуризации функций, относящихся непосредственно к реализации самой ИС. Она содержит три уровня и четыре группы функциональных компонентов в каждом. Эти уровни следующие:

- компоненты служб и сервисов промежуточного слоя (MW);
- компоненты операционных систем или операционного слоя (OW);
- аппаратный слой (HW).

Функциональные группы компонентов в данной модели составляют:

- компоненты, обеспечивающие интерфейс с пользователем (*User* – «U»);
- компоненты, обеспечивающие все необходимые процессы в системе (*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 модель взаимосвязи открытых систем (*OSI/RM – Open System Interconnection/Reference Model*).

Кроме того, модель трехмерна, она имеет несколько плоскостей. Для исследований рассматривались 3 плоскости: передняя базовая <ИС>, администрирования <А> и защиты <З>, которые могут отражать, каждая в своем контексте, функциональность базовой плоскости. К сожалению, защитная плоскость в стандарте [2] практически никак не прописана, поэтому дальнейшее представление плоскости защиты возможно в 2-х аспектах:

1. «Клетки» плоскости <З> интегрируют совокупности механизмов, обеспечивающих защиту реализаций соответствующих «клеток» базовой плоскости <ИС> – межкатегорийный аспект (в терминах стандарта [2]);
2. Поскольку КСЗ сама является информационной системой, то ее функциональность, в свою очередь, тоже может быть структурирована в соответствии с базовым представлением <ИС> с поправкой на контекст.

Результаты, представленные в данной работе, ориентированы на межкатегорийный аспект. Тогда задача обеспечения безопасности для ОЗ, представленного в виде модели *OSE/RM*, заключается в том, чтобы свойства *K, C, D* выполнялись для информационных и вычислительных ресурсов реализаций каждой «клетки» модели. Причем речь идет и о базовой плоскости <ИС>, структурирующей функции ИС, и о плоскости администрирования <А>, и о ресурсах самой системы безопасности, скомпонованных на плоскости защиты <З>. Очевидно, что цели *K, C, D* референсные, т.к. во-первых, они прикладываются к референсным функциональным группам, а во-вторых, для реализаций разных «клеток» модели их интерпретация различна. На рис.2 приведен пример интерпретации указанных свойств для «клеток» «Экранные формы приложения» и «Процессы системно-прикладного слоя».

Экранные формы

К: ограничение доступа к экранным формам приложения:

- ограниченный физический доступ любого пользователя к экрану компьютера, на котором отображаются формы;
- ограниченный доступ к приложению в части его экранных форм.

D: возможность отобразить формы на экране дисплея:

- физическая возможность,
- возможность, противостоящая спаму и вирусам,
- отсутствие блокировки формы.

C: способность сохранять экранные формы в том виде, в каком они были созданы.

Процессы системно-прикладного слоя

К: ограничение доступа со стороны соответствующих API-функций приложения к процессам системно-прикладного слоя;

D: возможность системному процессу или API-функции бизнес-логики обратиться к системно-прикладному процессу.

C: контроль целостности процессов.

Рис. 3. Пример интерпретации целей безопасности для разных «клеток» модели OSE\RM

Структуризация механизмов защиты

Далее задача заключалась в том, чтобы защитные механизмы *Mx* (как существующие на сегодняшний день, так и потенциально-возможные) структурировать в соответствии с целями «клеток» с учетом интерпретации. Тем самым будет обеспечено требование межкатегорийного представления плоскости <З>, декларируемое стандартом [2]. Анализ *Mx* позволил сделать вывод о том, что все множество механизмов можно разделить на 3 группы:

Группа 1. Целевые – обеспечивающие целевую функцию $\{\overline{KS}\} = \{C, D, K\}$. Эти *Mx* должны быть поставлены в соответствие реализациям «клеток» всех трех плоскостей, т.е. в идеале каждая «клетка» должна быть «закрыта» механизмами управления доступом, контролем целостности, обеспечением доступности.

Группа 2. Обеспечивающие, т.е. те, которые осуществляют дополнительные действия, необходимые для а) организации функционирования целевых *Mx* и б) осуществления целевым механизмом своего назначения на том или ином уровне безопасности. Например, чтобы обеспечить конфиденциальность файла данных, для которого установлены те или иные права доступа, система безопасности должна убедиться, что субъект, например, пользователь, обращающийся к нему, обладает соответствующим правом. Для этого необходимо задействовать, прежде всего, механизм организации сеанса с ИС, чтобы предоставить возможность пользователю обратиться к системе; затем механизмы идентификации, аутентификации пользователя; потом – механизм управления доступом к файлу, который и сопоставит права субъекта и файла. А чтобы обеспечить конфиденциальность на определенном уровне, надо использовать алгоритмы шифрования механизма криптоподдержки соответствующей стойкости.

Таким образом, каждый *Mx* из группы 1 требует поддержки обеспечивающих защитных механизмов. Табл. 1,2 демонстрируют пример взаимосвязи целевых и обеспечивающих *Mx* с точки зрения действий а), б). Подобные таблицы могут быть сформированы и согласованы экспертами предварительно.

Таблица 1 соответствия обеспечивающих и целевых Mx по конфиденциальности\целостности

Обеспечив. Mx	Организация сеанса	Идент-я, аутент-я	Доверенный канал	Криптоподдержка	Приватность данных	Разделение домена	Уничтожение остаточных данных
Критерий							
Конфиденциальность \целостность данных <ИС>	+\ [+]	+\[+]	+\+	+\+	+		+
Конфиденциальность \ целостность данных <З>	+\ [+]	+\[+]	+\+	+\+	+	+	+
Конфиденциальность \целостность данных <А>	+\ [+]	+\[+]	+\+	+\+	+		+

Таблица 2 соответствия обеспечивающих и целевых Mx по доступности

Обеспечив. Mx	Отказоустойчивость	Обслуживаемость	Восстановление данных	Откат данных	Резервирование
Критерий					
Доступность данных <ИС>	+	+	+	+	+
Доступность данных <З>	+	+	+	+	+
Доступность данных <А>	+	+	+	+	+

Следует заметить, что каждый *Mx* из группы референсный и представляет собой иерархию механизмов-подклассов, обладающих многими атрибутами; их действие направлено на разные объекты ИС. Для дальнейшей структуризации необходимо представить внутреннюю структуру *Mx* в виде некоторой модели. Для этой цели были использованы семантические модели в виде онтологий. На рис. 3 представлена онтология общего представления класса механизмов защиты {Mx} и экземпляр одного из целевых механизмов – управления доступом.

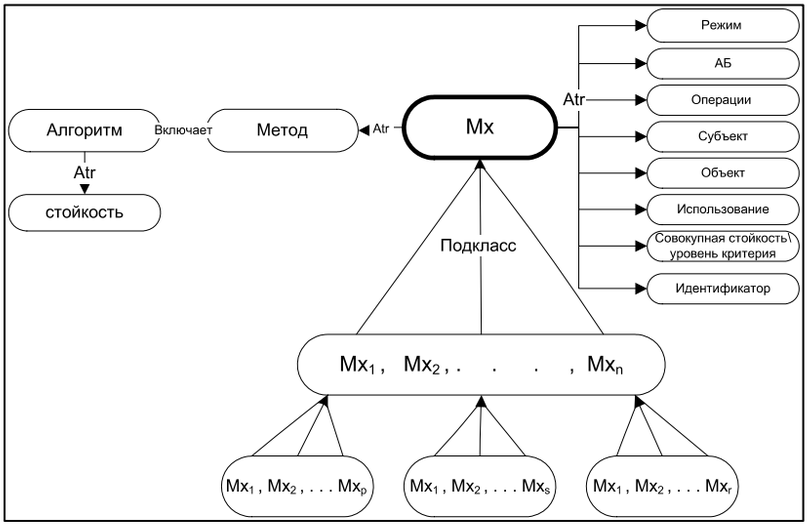

Рис. 3-а. Онтологии класса защитные механизмы {Mx}

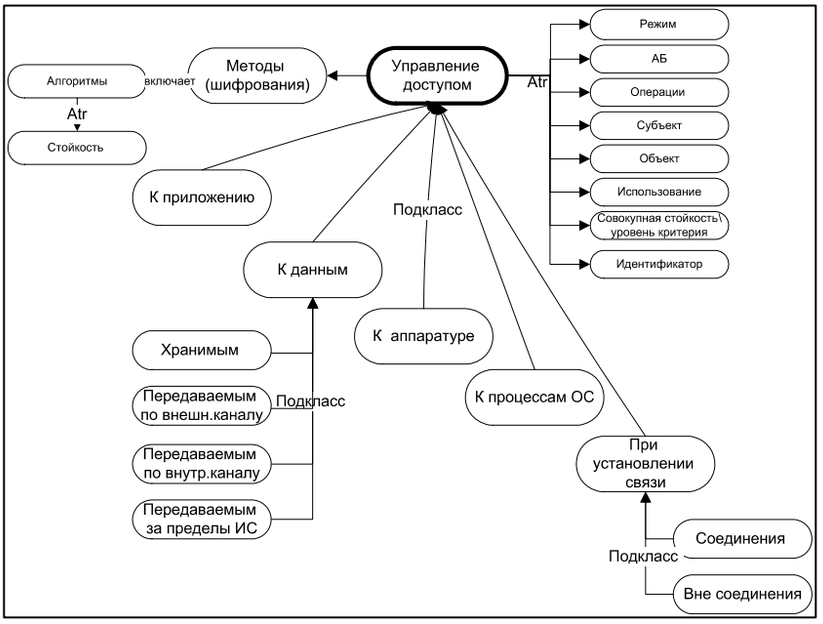

Рис. 3-б. Онтологии механизма управления доступом

Дальше идея заключается в том, чтобы соотнести листья таксономий целевых *Mx* с «клетками» ОЗ, а листья обеспечивающих *Mx* – сопоставить с целевыми в соответствии с таблицами 1,2. Реализация управляющих механизмов осуществляется в виде приложения системы защиты. Тем самым выстраивается референсная модель КСЗ для ИС. Следует заметить, что это – общая универсальная модель. Однако она дает понимание того, как выстраивать бизнес-процессы защиты ИС исходя из конкретных потребностей, диктуемых реализацией ИС и политиками безопасности организаций.

Референсное описание базового подмножества бизнес-процессов защиты

В любой информационной системе над данными производятся несколько типичных операций: ввод\вывод, хранение, обработка, передача на съемные носители, передача через локальную или глобальную сеть. Именно на защиту этих операций, прежде всего и нацелен национальный стандарт в области информационной безопасности [5]. При этом в качестве данных рассматриваются как пользовательские массивы, ассоциированные с базовой плоскостью <ИС>, так и данные по администрированию системы (плоскость <А>) и безопасности (плоскость <З>).

Все эти виды операций реализуются средствами тех или иных «клеток» модели и их можно представить в виде последовательности переходов по «клеткам».

1. Хранение данных предполагает организацию (высокоуровневую или низкоуровневую) данных, представление в виде некоторого формата, хранение на диске, осуществляется для:

a. пользовательских массивов – хранение осуществляется средствами «клеток» столбца <ИС><HW>< I >.

b. системных данных – <А><HW>< I >.

c. данных системы безопасности – <З><HW>< I >.

Следует отметить, что все три типа данных в реальности могут храниться на одном диске.

2. Обработка данных, осуществляется посредством функционирования процессов, инициированных приложением, например:

a. Вычисления – операции, производимые над содержимым ячеек оперативной памяти. Инициируется алгоритмом приложения – «клетка» <ИС><Appl><S>, затем процесс <ИС><OW><S> обращается к содержимому оперативной памяти <ИС><HW><I>, в процессоре осуществляется арифметика над данными (<ИС><HW><S>) и результат возвращается в оперативную память <ИС><HW><I>.

b. Модификация – операции, производимые над уже существующими полями записи файлов, БД.

3. Ввод\вывод данных: копирование данных из входного потока или файла в ячейки ОП и поля записи\из ячеек и полей в выходной поток или файл, осуществляемые приложением.

4. *Передача данных (прикладных, административных, безопасности), реализуемая через съемные носители (клетки U, I строки HW*). Такая операция может производиться по инициативе непосредственно пользователя, тогда она осуществляется средствами ОС, например, копирование данных на дискету или вывод файла на принтер. Эта инициация начинается в «клетке» <ИС><OW><U>, далее запускается процесс в «клетке» <ИС><OW><S>, который обращается к файловой системе <ИС><OW><I>, происходит чтение данных с жесткого диска <ИС><HW><I> и там же запись на дискету или передача на принтер <ИС><HW><U> по пунктирной стрелке.

Если пользователь осуществляет те же операции, используя приложение, то процесс начинается через форму приложения («клетка» <ИС><Appl><U>), которая запускает ветвь алгоритма <ИС><Appl><S> и далее по стрелкам.

Аналогично работает и цепочка ввода данных. При этом данные также могут быть как пользовательскими, так и служебными, просто тогда они берутся из соответствующих «клеток» плоскостей <А> или <З>.

5. *Передача данных (прикладных, административных, безопасности), которая происходит через локальную или внешнюю сеть (столбец С).* Осуществляется посредством установки взаимодействия между узлами сети.

Операция состоит из нескольких этапов:

– Подготовка – инициация взаимодействия (соединения), происходит по требованию пользователя, но осуществляться может средствами ОС («клетка» <ИС><OW><U>) либо посредством прикладного приложения (<ИС><Appl><U>).

– Установка удаленного соединения с внешней ИС или по локальной сети, инициируется средствами «клетки» <ИС><MW><S>.

– Подкачка данных из БД для передачи.

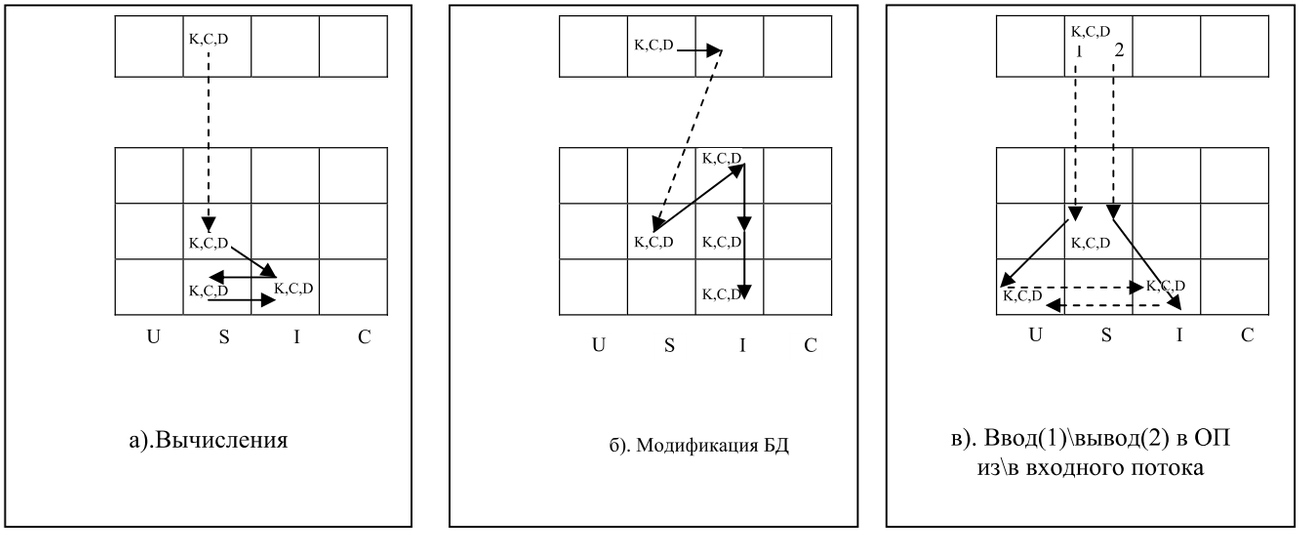

Рис. 4. Представление операций обработки данных посредством вычислений (а), модификации БД (б) и ввода\вывода из входного потока (в)

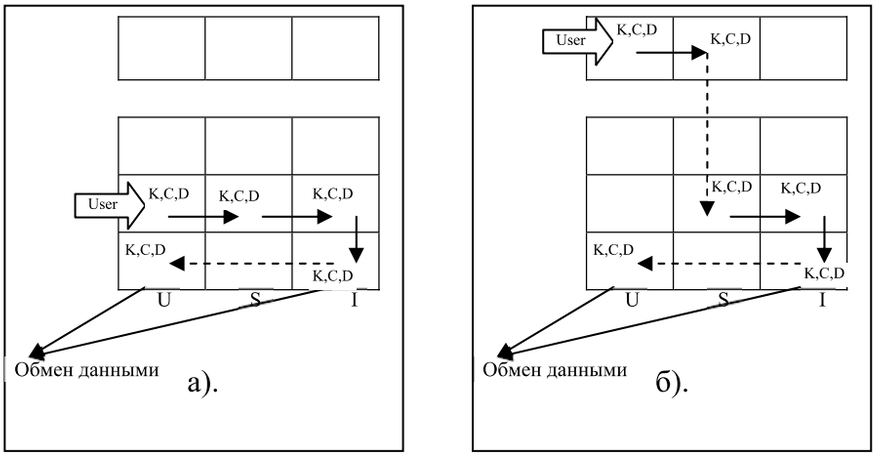

Рис. 5. Передача данных на съемные носители, инициируемый пользователем с использованием средств ОС (а) или формы приложения (б)

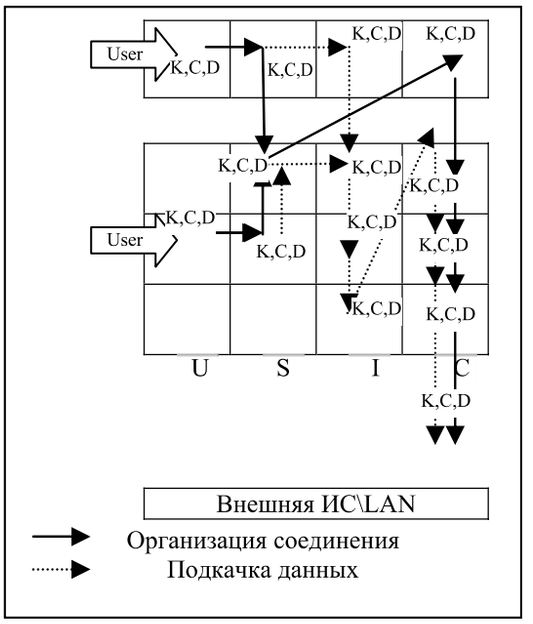

Рис. 6. Передача данных через локальную или глобальную сеть

Именно под описанные операции на сегодняшний день и разработаны *Mx*, хотя очевидно, что при наличии соответствующих средств реализации механизмов референсное представление функциональности плоскости <З> дает возможность подобрать *Mx* под любую операцию, осуществляемую в системе. Разумеется, в системе происходят не только указанные операции, но достоинство в том, что референсное представление функциональности плоскости <З> дает возможность подобрать *Mx* под любую операцию, осуществляемую в системе.

Стало быть, именно «клетки», задействованные в операции, и должны быть «закрыты» защитными механизмами, а последовательность «клеток», которым поставлены в соответствие цепочки целевых и обеспечивающих механизмов, и представляют собой бизнес-процесс защиты. Рисунки 4-6 демонстрируют базовое подмножество бизнес-процессов защиты, построенных на основе типичных операций над данными, описанных выше.

Заключение

В заключение подчеркнем, что же дает представление информационной системы в виде модели *OSE\RM* для проектирования системы защиты:

1. Систематизированный комплексный взгляд на ИС, как на объект защиты.

2. Трехмерность модели позволяет представить все грани ИС – базовую, администрирования, защитную – в виде единой системы.

3. Систематизированное представление функциональности ИС любой сложности, от отдельного компьютера до территориально-распределенных систем, включая защитную плоскость, *позволяет стандартизовать систему безопасности*, т.е. сопоставить «клеткам» плоскости защиты множества стандартов или спецификаций, регламентирующих как проектирование системы защиты, так и ее эксплуатацию.

4. Специфицированная функциональность реализации защитного компонента в виде межкатегорийных сервисов (механизмов), структурированных по *OSE\RM*, *дает возможность приобрести*

системе безопасности свойства открытости [3,4], а именно: расширяемости, масштабируемости, мобильности приложений, мобильности пользователей, интероперабельности.

5. Декомпозиция целей безопасности $\overline{KS}(C, D, K)$ по «клеткам» модели дает возможность конструировать референсные бизнес-процессы защиты, которые позволяют получать обоснованные требования к приложениям в рамках КСЗ относительно реализаций «клеток» – объектов ИС.

Литература

1. **Калянов Г.Н.** Моделирование, анализ, реорганизация и автоматизация бизнес-процессов. М.: Финансы и статистика, 2006 г. – 240 с..

2. ISO/IEC TR 14252-1996 Guide to the POSIX Open System Environment.

3. ГОСТ Р ИСО/МЭК ТО 10000-1-2-3-99. Информационная технология. Основы и таксономия международных функциональных стандартов.

4. **Бойченко А.В., Кондратьев В.К, Филинов Е.Н.** Основы открытых информационных систем. 2-е изд. – М. : МЭСИ., 2004 г.

5. ГОСТ Р ИСО/МЭК 15408-2009. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.