А. Л. Антипов, А. И. Труфанов (к. т. н., доцент)
Иркутский государственный технический университет

МОДЕЛЬ ДИНАМИЧЕСКОЙ АДАПТИВНОЙ ИЕРАРХИЧЕСКОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В методологии нелинейной динамики предлагается модель адаптивной системы информационной безопасности. Исследуется и строится решение задачи оптимизации защиты информационных потоков. Исповедуемые принципы позволяют наглядно оценить системы безопасности на достаточном для изучения временном промежутке.

Постановка задачи

Повышение эффективности деятельности любого предприятия зависит прежде всего от эффективности использования информационных ресурсов. В свою очередь, эффективность использования информации напрямую связана с проблемой ее защиты. В рамках предприятий можно говорить о существовании множества разнотипных информационных потоков, требующих защиты. Используемые в настоящее время для организации систем информационной безопасности (далее — ИБ) статические модели имеют существенный недостаток, связанный с использованием в качестве базиса принципа статичности. Статичность с течением времени приводит к нарушению закона необходимого разнообразия Эшби [1]. Адаптированная формулировка данного закона для систем защиты может иметь вид: «Разнообразие мер защиты всегда должно превышать или как минимум быть равным разнообразию угроз».

Следствием нарушения закона необходимого разнообразия Эшби являются:

· снижение защищенности информационной системы;

· снижение общего быстродействия системы;

· ограничения по доступу к системе пользователей;

· задействование значительных вычислительных ресурсов.

Вследствие этого зачастую на настоящий момент имеет место отказ от построения единой системы ИБ в рамках предприятий и организация защиты, состоящей из набора относительно простых автономных подсистем, каждая из которых действует в одном или нескольких, но не во всех информационных каналах. Таким образом, актуальной является разработка новых подходов к построению и управлению системами ИБ с целью оптимизации быстродействия всей информационно-вычислительной системы и минимизации используемого для этого вычислительного ресурса.

Иными словами, ставится задача построения системы защиты, отвечающей следующим требованиям:

· максимальность уровня защиты

— надежность и бесперебойность защиты,

— стабильность,

— самоорганизованность,

— своевременность обеспечения защиты;

· минимальность уровня нагрузки на информационную систему предприятия;

· максимальность эффективности и экономичности функционирования защиты.

Формулировка модели безопасности

С точки зрения общей теории систем [2] задача организации защиты информационно-вычислительной системы может быть сформулирована как оптимизация процесса взаимодействия защитной подсистемы со всей системой и ее внешним окружением (в биологии аналог этому — иммунная система организма). То, что такая аналогия уместна, можно понять, если проанализировать направленность работы иммунной системы биологического организма. Иммунная система биологического организма нацелена на защиту системы (если под системой принять в данном случае биологический организм) [3]. Самое поразительное свойство иммунной системы — то, что она может реагировать на миллионы чужеродных антигенов, вырабатывая антитела, специфически взаимодействующие с антигенами. Кроме этого, иммунная система способна вырабатывать антитела к молекулам, созданным человеком и не существующим в природе.

Для построения модели системы ИБ, описывающей во времени формирование ответа системы на угрозы, предлагается использовать концепцию построения иммунного ответа биологического организма на вводимый антиген [4].

Модель представляет собой систему кинетических дифференциальных уравнений второго рода с насыщением, которые описывают систему защиты, вырабатываемые контрмеры, угрозы. Выбор математического аппарата для описания модели был сделан в пользу дифференциального исчисления и нелинейной динамики [5, 6] по следующим причинам:

— возможность динамически отслеживать реакцию системы обеспечения информационной безопасности на угрозы различной природы;

— относительная простота описания модели с помощью дифференциального исчисления по сравнению с математическим аппаратом теории игр;

— возможность практического применения.

Основное свойство модели — динамическое развертывание активной защиты на период выполнения конкретных задач по защите информации.

При отсутствии внешней угрозы система защиты свернута до одного уровня. При таком состоянии системы защиты обеспечивается базовый уровень защищенности. В случае появления угрозы система защиты разворачивается до трехуровневой иерархически выстроенной системы. Обозначим эти уровни по нисходящей: X, Y, Z. Построим дерево целей системы (Рис. 1.) согласно [2].

Итак, уровень X является базовым уровнем системы. На нем реализованы функции регулирования, функционирования и наблюдения за системой.

В случае появления угрозы элементы уровня X при взаимодействии с угрозой проводят ее оценку. Также уровень X управляет развертыванием нижестоящего уровня Y. Элементы уровня Y, повторно взаимодействующие с угрозой, вырабатывают решения о развертывании уровня Z. Элементы системы уровня Y, которые повторно не взаимодействовали с угрозой, служат источником информации по данной угрозе. Элементы уровня Z отвечают за выработку контрмер.

Под угрозами понимаются возможности возникновения ущерба от взаимодействия факторов угроз с подсистемами и связями субъектов безопасности (трактовка Остапенко Г. А. [7]).

Целесообразно рассматривать следующие типы связей между уровнями системы ИБ (Рис. 2):

канал c1 — наблюдение за системой и ее окружением;

канал c2 — взаимодействие с угрозой элементов уровня X;

канал c3 — передача управляющей информации на уровень Y;

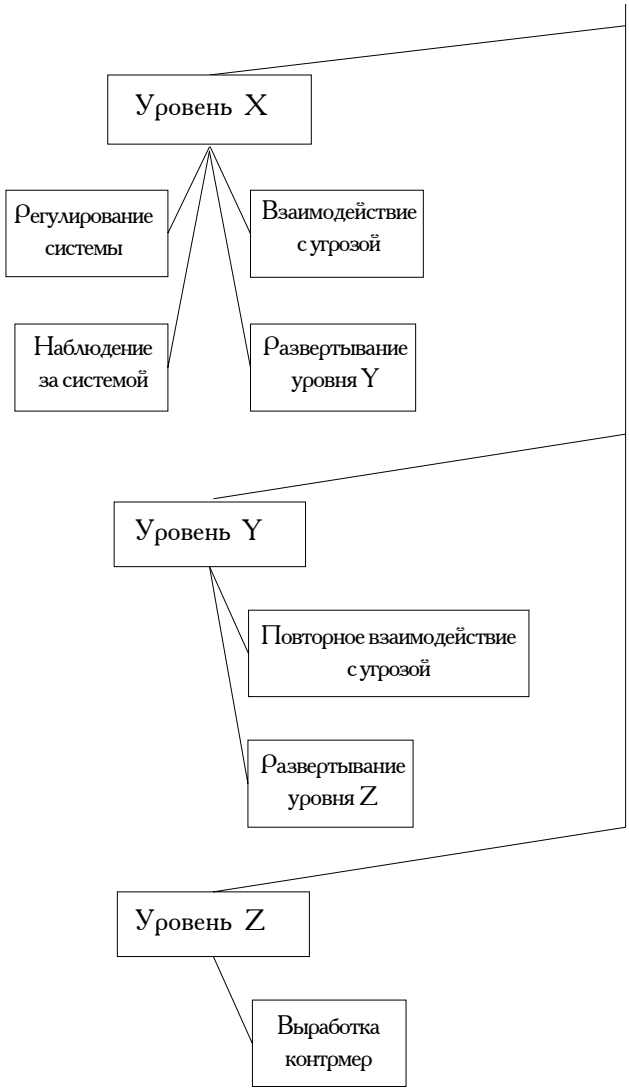

Рис. 1. Дерево целей системы

канал с4 — передача информации об угрозе на уровень Y;
канал с5 — взаимодействие с угрозой элементов уровня Y;
канал с6 — передача управляющей информации на уровень Z;
канал с7 — передача информации об угрозе на уровень Z;
канал с8 — канал взаимодействия контрмеры с угрозой.

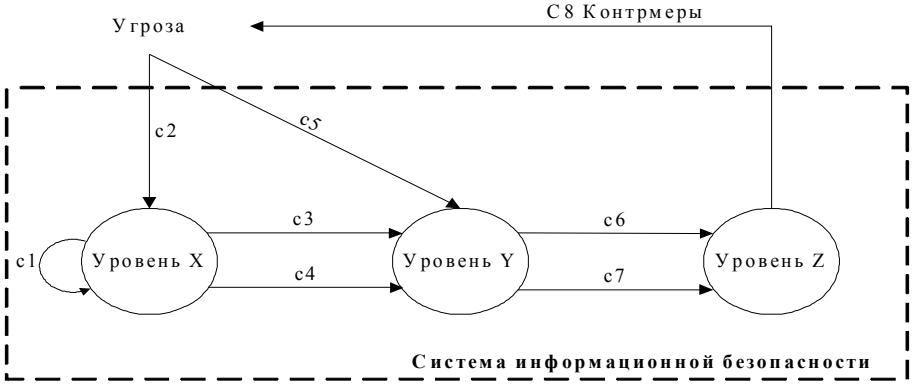

Рис. 2. Типы связей

Модель системы безопасности имеет следующий вид:

$$\frac{dX}{dt} = v - \alpha_x XG - \kappa_x X,$$
$$\frac{dY}{dt} = \alpha_x XG + \mu(G)Y - \alpha_y YG - \kappa_y Y,$$
$$\frac{dZ}{dt} = \alpha_y YG - \kappa_z Z, \qquad (1)$$
$$\frac{dG}{dt} = -\kappa_g G - \alpha_{gf} GF,$$
$$\frac{dF}{dt} = h_z Z - \alpha_{gf} GF - \kappa_f F,$$

где v – скорость появления новых элементов на уровне X и k_i (i=x, y, z) – коэффициент уничтожения устаревших элементов уровня (коэффициент старения).

Развертывание нижестоящего уровня пропорционально вероятности взаимодействия элементов уровня X, Y с угрозой: для уровня X – $\alpha_x XG$ для уровня Y – $\alpha_y YG$ где α_i $(i=x,y)$ – коэффициент взаимодействия элементов уровня X, Y с угрозами.

Рост количества элементов уровня Y будет идти со скоростью $\mu(G)$. Функцию $\mu(G)$ можно аппроксимировать гиперболой:

$$\mu(G) = \mu_0 G (k_g + G)^{-1} \qquad (2)$$

т. е. постановить, что при G=0 не происходит наращивание уровня Y, а при увеличении уровня угрозы скорость нарастания количества элементов уровня Y увеличивается, но не может стать больше некоторого фиксированного значения μ_0.

Величины k_g и k_f характеризуют времена устаревания угроз (устаревания применяемых контрмер), h_z – скорость выработки контрмер элементами уровня Z, α_{gf} – коэффициент взаимодействия контрмера–угроза.

Обозначим через:

$$X(Y,Z) = \frac{\sum_{x(y,z)=1}^{n} x(y,z) * \varphi_{x(y,z)}}{\sum_{i=1}^{m} C_i} \text{ – насыщенность элементами на уровне,} \qquad (3)$$

где x – количество элементов одного типа на уровне X, φ_x – вес типа элементов, C_i – вес информационного узла, где установлен элемент. Аналогичным образом обозначим насыщенности элементами на уровнях Y, Z.

Для насыщенности угроз: g – количество угроз одного типа, φ_g – вес угроз одного типа, воздействующих на информационную систему, C_i – вес информационного узла, на который воздействует угроза.

$$G = \frac{\sum_{g=1}^{n} g * \varphi_g}{\sum_{i=1}^{m} C_i} \text{ – насыщенность угроз.} \qquad (4)$$

Для насыщенности контрмер: f – количество контрмер одного типа, применяемых в информационной системе, φ_f – вес контрмер одного типа, C_i – вес защищаемого информационного узла.

$$F = \frac{\sum_{f=1}^{n} f * \varphi_f}{\sum_{i=1}^{m} C_i}$$ — насыщенность используемых контрмер. (5)

Согласно [4], система должна отвечать следующему условию: $S > \sum_{i=1}^{3} S_i$, (6)

где S_i — эффективность функционирования i-х уровней системы защиты; S — эффективность функционирования системы защиты, т. е. интегральный ресурс системы должен быть больше суммы ресурсов составляющих ее элементов.

Доказательство выполнения данного неравенства можно найти в работе [8], где доказывается тот факт, что интегральная эффективность многоуровневой иерархической системы всегда больше эффективности составляющих ее уровней.

Основные результаты

При оценке параметров модели воспользуемся подходами, развитыми в «модели искусственной иммунной антивирусной системы» корпорации IBM [9], в работах [10, 11].

Для упрощения расчетов исключим возможный кооперативный эффект действия атаки, т.е. будем считать, что угрозы воздействуют на каждый элемент системы защиты индивидуально. Тогда коэффициенты взаимодействия с угрозами будут отражать скорость противодействия системы защиты атакующим воздействиям. Примем, что диапазон возможных υ (скорость появления новых элементов на уровне X) = 0..1, диапазон возможных h_z (скорость выработки контрмер элементами уровня Z) = 0..1, диапазон возможных μ_0 (удельная скорость появления элементов на уровне У) = 0..1. Нулевым порогом будем считать условие, что уровень насыщенности опустился до 10^{-4}.

Исследование модели системы обеспечения информационной безопасности в формализме фазовых траекторий проводилось в несколько этапов.

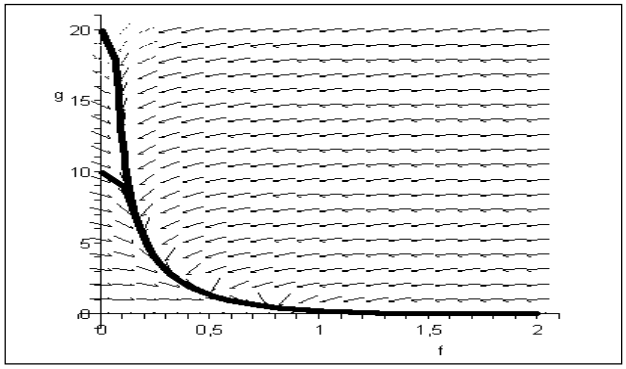

Рис. 3. Фазовые портреты частной двумерной модели системы «Угрозы—Контрмеры»

На первом этапе исследовалась частная двумерная модель системы «Угрозы—Контрмеры» (фиксация трех из пяти переменных). На рис. 3 представлены примеры фазовых портретов такой модели системы ИБ при уровне насыщенности угроз G=10, 20. Для данной частной двумерной модели системы «Угрозы—Контрмеры» характерно малое изменение фазового портрета при существенном изменении начальных условий. Использование двух переменных (угрозы и контрмеры) недостаточно для полного описания работы системы ИБ. Данная частная модель может найти применение только для динамического описания выбора решений при противоборстве с атакующим.

На втором этапе проводились исследования следующих трехмерных моделей системы ИБ (фиксация двух из пяти переменных):

· системы ИБ «X-Y-Z» — постоянный уровень насыщенности угроз и контрмер;

· системы ИБ «Y-Z-G» — постоянный уровень насыщенности элементами на уровне X и насыщенности контрмер;

· системы ИБ «Y-Z-F» — постоянный уровень насыщенности элементами на уровне X и насыщенности угроз.

На рис. 4—5 представлены примеры наиболее вероятных фазовых траекторий частных трехмерных систем ИБ (система безопасности «X-Y-Z» — постоянный уровень насыщенности угроз и контрмер X, Y, Z; системы ИБ «Y-Z-G» — постоянный уровень насыщенности элементами на уровне X и насыщенности контрмер).

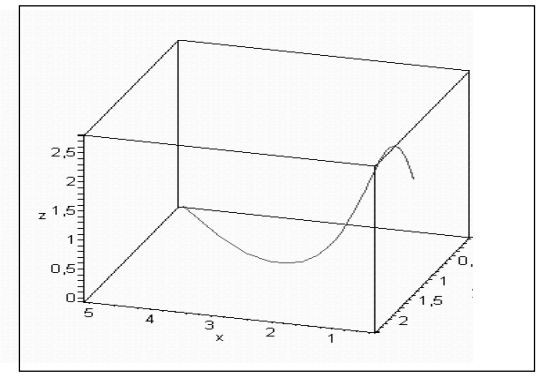

Рис. 4. Фазовая траектория частной трехмерной системы ИБ «X-Y-Z»

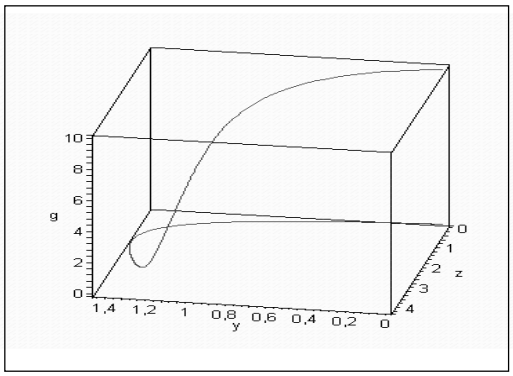

Рис. 5. Фазовая траектория частной трехмерной системы ИБ «Y-Z-G»

Исследования представленных выше частных трехмерных моделей системы ИБ были проведены с целью изучения динамики реакции трехуровневой иерархической системы защиты на критические условия. Частная модель системы ИБ «X-Y-Z» может быть использована для определения в дальнейшем чувствительности системы защиты (анализ пассивной обороны). Исследование модели системы ИБ «Y-Z-G» показало, что изменение количества и качества элементов уровня X и вырабатываемых контрмер приводит к неоднородности построения системы ИБ. Т.е. основная сложность в разработке и поддержании систем ИБ приходится на 1-й уровень систем защиты.

На третьем этапе было проведено исследование системы ИБ «X-G-F», имеющей один уровень защиты. Расчеты по данной модели показали, что существенным фактором, снижающим эффективность данной системы, кроме указанного в [8], является поддержание на постоянном уровне насыщенности контрмер уже после решения задачи нейтрализации угроз. Также было выявлено, что время достижения равновесия в подобной системе ИБ существенно больше времени достижения положения равновесия в частных трехмерных моделях системы ИБ.

На последнем этапе было проведено исследование полной пятимерной модели системы ИБ. При исследовании предлагаемой модели системы на устойчивость по Ляпунову получено доказательство возможности существования подобной системы ИБ. На рис. 6—10 представлены графики изменения насыщенности элементами на уровнях (X, Y, Z), изменения насыщенности контрмер, угроз при следующих начальных условиях: скорость появления элементов на уровне X = 0.5; насыщенность элементами на уровне X = 1; коэффициент взаимодействия элементов уровня системы защиты (X, Y) с угрозой = 0.5; коэффициент старения элементов уровня (X, Y, Z) = 0.5; насыщенность угрозами = 5; насыщенность контрмерами = 0; скорость прироста насыщенности контрмерами = 0.5; коэффициент взаимодействия «Угроза—Контрмера» = 0.5; коэффициент старения угроз/контрмер = 0.05; $\mu_0 = 0$. На рис. 11 представлена наиболее вероятная фазовая траектория по срезу «Угрозы—Контрмеры» модели системы ИБ.

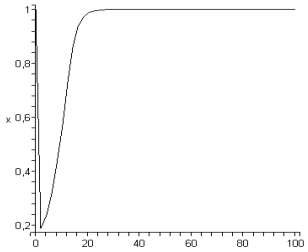

Рис. 6. График X(t)

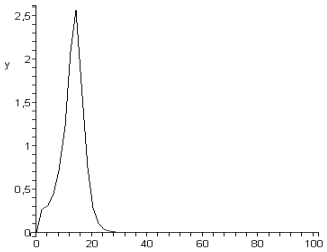

Рис. 7. График Y(t)

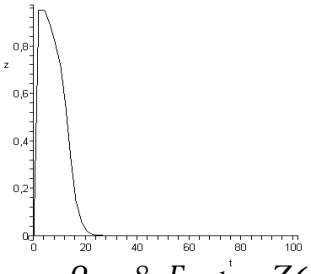

Рис. 8. График Z(t)

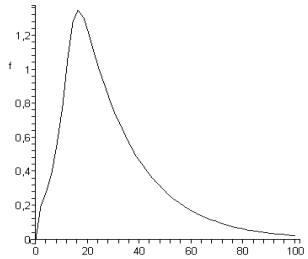

Рис. 9. График F(t)

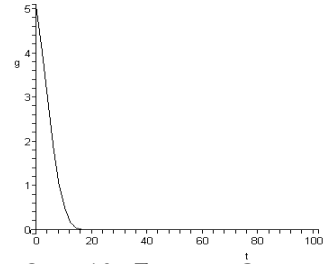

Рис. 10. График G(t)

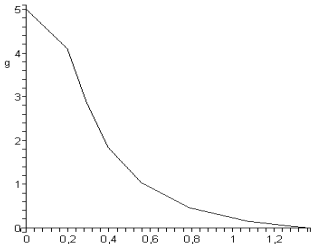

Рис. 11. Фазовая траектория по срезу «Угрозы—Контрмеры»

Таким образом, несмотря даже на пятикратное превышение насыщенности угроз над насыщенностью элементами системы защиты, в начальный момент времени нейтрализация угроз происходит менее чем за 20 условных промежутков времени. Это доказывает существенную стойкость предлагаемой модели системы ИБ к высокому уровню угроз.

Выводы

Разработка *модели динамической адаптивной системы обеспечения информационной безопасности и первые результаты исследований с ее применением позволили установить следующее*:

· Изначальное преимущество предлагаемого подхода к разработке, контролю и оцениванию систем ИБ заключено в использовании принципа динамичности и, следовательно, строгом соответствии закону необходимого разнообразия Эшби. Разработанная динамическая модель иерархической системы ИБ предлагает решение задачи оптимизации защиты информационных потоков.

· Методология нелинейной динамики позволяет наглядно и с достаточной степенью достоверности оценить системы ИБ на достаточном для изучения временном промежутке.

· Дополнительные простые экономические оценки указывают на то, что система ИБ, построенная на предлагаемых принципах, имеет более высокий уровень защищенности информационных ресурсов при более низкой совокупной стоимости владения.

· Скорость реакции системы защиты зависит в первую очередь от скорости развертывания 2-го и 3-го уровней защиты.

СПИСОК ЛИТЕРАТУРЫ:

1. *Росс Эшби У.* Введение в кибернетику. М., 2006.
2. *Шилейко А. В., Кочнев В. Ф., Химушин Ф. Ф.* Введение в информационную теорию систем / Под ред. А. В. Шилейко. М., 1985.
3. *Албертс Б., Брей Д., Льюис Дж., Рэфф М., Робертс К., Уотсон Дж.* Молекулярная биология клетки: в 3-х т. 2-е изд., перераб. и доп. Пер. с англ. М., 1994.
4. *Романовский Ю. М., Степанова Н. В., Чернавский Д. С.* Математическая биофизика. М., 1984.

5. *Данилов Ю. А.* Лекции по нелинейной динамике. Элементарное введение. М., 2001.
6. *Карлов Н. В., Кириченко Н. А.* Колебания, волны, структуры. М., 2001.
7. *Остапенко Г. А.* Информационные операции и атаки в социотехнических системах. Учебное пособие для вузов / Под ред. чл.-корр. РАН В. И. Борисова. М., 2007.
8. *Капица С. П., Курдюмов С. П., Малинецкий Г. Г.* Синергетика и прогнозы будущего. М., 1997.
9. *Jeffrey O. Kephart*. A Biologically Inspired Immune System for Computers, High Integrity Computing Laboratory IBM Thomas J. Watson Research Center // http://www.ibm.com.
10. *Труфанов А. И.* Балансовая модель производства информационных ресурсов в условиях конкурентной борьбы // Проблемы равновесия и устойчивости в экономических и социальных системах. Сб. науч. тр. Новосибирск, 1999.
11. *Герасименко В. А., Малюк А. А.* Основы защиты информации. М., 1997.

И. О. Атовмян (д. т. н., профессор)
Московский инженерно-физический институт (государственный университет)
В. С. Лаврентьев (к. т. н., доцент)
Московский инженерно-физический институт (государственный университет)

О РЕАЛИЗАЦИИ МОДЕЛИ КОНТРОЛЯ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ В БАЗЕ ДАННЫХ (МОДЕЛИ БИБА) СРЕДСТВАМИ СУБД Oracle

В статье приводится решение задачи практической реализации модели Биба комплексным использованием различных средств СУБД Oracle, в которой на сегодняшний день не предусмотрены специальные средства мандатного контроля целостности.

Части реляционной модели, связанной с обеспечением целостности информации, уделяется в последние годы серьезное внимание [1]. Вместе с тем для такой базовой модели разграничения целостности, как модель Биба [2, 3], готовых решений на сегодняшний день в существующих СУБД нет. Авторы предлагают возможный вариант решения задачи мандатного метода разграничения целостности (соответствующего модели Биба) — на примере СУБД Oracle10gEE.

Напомним, что модель Биба устанавливает уровни целостности для субъектов (пользователей информации) и объектов (таблиц базы данных).

Обозначения на рис. 1: Sh — субъект с высоким уровнем целостности, Oh — объект с высоким уровнем целостности, Si и Oi — соответственно субъект и объект с низким уровнем целостности [3].

Первый вопрос, который приходится решать при реализации модели Биба, как, впрочем, и любой другой модели контроля целостности: чем конкретно различаются уровни целостности объектов.

Если объекты — разные таблицы, тогда различие уровней целостности может определяться разным набором constraint — правил ограничения целостности таблиц (primary key, foreign key, unicum key, constraint NOT NULL и т. д.), разным набором триггеров, обеспечивающих специфические проверки. Для одной таблицы это может быть расширенный набор constraints и триггеров (Oh) , для другой — суженный (Oi). И тогда модель Биба, это очевидно, реализуется группой объектных привилегий, в число которых входят привилегии read, write — в сочетании с требуемыми триггерами. Здесь все просто.