УДК 004.056.53+004.056.57

В.В. Грызунов

Аналитическая модель целостной информационной системы

Представлена и прокомментирована аналитическая модель целостной информационной системы. Показано, что вопросы защиты информации в информационной системе, обладающей целостностью, не актуальны.

Ключевые слова: защита информации, безопасность информационной системы, модель информационной системы, целостность, взаимодействие уровней информационной системы.

На любом предприятии информационная система (ИС) является стратегически и тактически важным объектом, так как от её работоспособности зависит полнота и целесообразность использования ресурсов предприятия. Можно сказать, что с помощью ИС координируются и согласуются действия других элементов предприятия, контролируется использование и распределяются ресурсы предприятия. Именно поэтому контроль над ИС является основной целью злоумышленников [1]. Обеспечение безопасности ИС позволяет гарантировать, что ресурсы предприятия используются в интересах его владельцев, а не в интересах злоумышленников, получивших несанкционированных доступ к ИС. Обеспечение безопасности ИС имеет ряд особенностей, присущих ИС как иерархической системе.

ИС представляет собой сложный объект, имеющий несколько уровней иерархии. Условно эти уровни можно представить так, как это показано на рисунке 1. Распространим утверждения, приведённые в [2], на ИС. Можно сказать, что каждый вышестоящий уровень является «метасистемой» для всех нижестоящих уровней, т.е. «аксиомой», задающей основные требования к множеству допустимых (возможных) и требуемых пространственно-временных состояний нижестоящих уровней. «Аксиомой, не требующей доказательств», для программного обеспечения (ПО) является аппаратное обеспечение (АО), для аппаратного обеспечения – действия персонала (П). Персонал, в свою очередь, должен действовать в соответствии с условиями и ограничениями различных видов обеспечения (об).

Так, например, ПО, выполняясь, использует предоставленную процессором систему команд и может получить доступ только в те участки памяти, что разрешены процессором, а современные процессоры выделяют область памяти, куда запрещают доступ для всех программ.

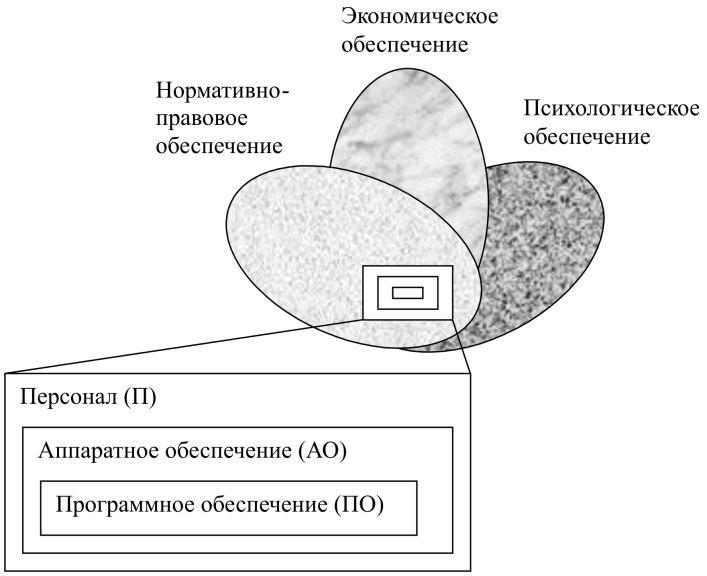

Рис. 1. Уровни иерархии ИС

Само аппаратное обеспечение (и, соответственно, ПО) функционирует под управлением персонала, который подаёт электропитание, разграничивает доступ к оборудованию и т.д.

Говоря про персонал, необходимо отметить, что человек (персонал) по своей природе – биосоциальное существо, обладающее психикой. Соответственно, на него влияют как законы реального мира, так и нормы морали, юридические законы, экономические и психологические факторы, и т.п. Разные факторы влияют на разных людей по-разному. Например, неправомерный доступ к компьютерной ин-

формации или распространение вредоносных программ запрещено уголовным кодексом. Однако сильная нужда, тщеславие или жадность могут сделать более приоритетным получение экономической выгоды, и человек пойдёт на преступление. Или, например, введённый в состояние «зомби» человек будет беспрекословно выполнять инструкции злоумышленника. Человек – пока не изученное существо, и классификация элементов обеспечивающего уровня – предмет дополнительных исследований, поэтому далее, говоря об обеспечивающем уровне, будем иметь в виду лишь явно выделяющиеся нормативно-правовую, экономическую и психологическую составляющие.

В процессе штатного функционирования, каждый уровень должен представлять собой *целостную* систему [3, 4]. Это означает, что должно выполняться условие

$$\int_{Q^{Y}} \varphi^{Y}(r^{Y}) dr^{Y} = I^{Y}, \tag{1}$$

где Q^{Y} – множество требуемых пространственно-временных состояний уровня ИС;

$$r^{Y} = F(q \in Q^{Y});$$

I^{Y} – показатель эффективности применения уровня ИС;
$\varphi^{Y}(r^{Y})$ – потенциал поля эффективности (ППЭ) уровня – способность уровня решать поставленные задачи в r^{Y} (удельная производительность уровня в r^{Y});.

$$Y = \text{об, П, АО, ПО.}$$

Данное уравнение в общем виде имеет 2 переменных: Q и I. Фиксируя одну из переменных, мы получаем значение другой.

Поскольку работоспособность верхних уровней зависит от работоспособности нижних уровней $\varphi^{ИС}(r^{ИС}) = \varphi^{об}(r^{об}, \varphi^{П}(r^{П}, \varphi^{АО}(r^{АО}, \varphi^{ПО}(r^{ПО}))))$, то связь показателей эффективностей применения ИС различных уровней и множеств требуемых состояний уровней можно записать следующим образом:

$$\int_{Q^{об}} \int_{Q^{П}} \int_{Q^{АО}} \int_{Q^{ПО}} \varphi^{ИС}(r^{ИС})\, dr^{ПО} dr^{АО} dr^{П} dr^{об} = I^{ИС}, \tag{2}$$

при этом

$$Q^{об} \cup Q^{П} \cup Q^{АО} \cup Q^{ПО} = Q^{ИС},$$

поэтому с учётом (1) верно

$$I^{об}(I^{П}(I^{АО}(I^{ПО}))) = I^{ИС}, \tag{3}$$

где $Q^{об}$, $Q^{П}$, $Q^{АО}$, $Q^{ПО}$, $Q^{ИС}$ – соответственно, множества требуемых пространственно-временных состояний обеспечивающего уровня, персонала, аппаратного и программного обеспечений всей ИС,

$$R^{ИС} = F(Q \in Q^{ИС}),$$

$I^{об}$, $I^{П}$, $I^{АО}$, $I^{ПО}$, $I^{ИС}$ – соответственно, показатели эффективности применения обеспечивающего уровня, персонала, аппаратного и программного обеспечений, всей ИС,
$\varphi^{ИС}(r^{ИС})$ – способность ИС решать задачи в $r^{ИС}$.

Если для объекта верно равенство (2), говорят, что *объект обладает целостностью*.

В свою очередь, верхние уровни определяют, на что именно в их работе влияет и как будет учитываться эффективность применения нижнего уровня. Это решается при задании функции φ^{Y}. Определяя функцию φ^{Y}, верхний уровень накладывает ограничения (предъявляет требования) на множества требуемых состояний нижних уровней.

Из выражений (2) и (3) видно, что нижние уровни влияют на верхние посредством формирования своего показателя эффективности применения. Уровень может *непосредственно* взаимодействовать только с уровнем, ближайшим к нему. Это хорошо заметно при взаимодействии уровней «персонал» и «ПО». Человек не может непосредственно воздействовать на ПО, для этого ему нужно АО (клавиатура, мышь, стилус и т.д.). И, наоборот, ПО не может непосредственно передавать человеку результаты обработки данных без средств отображения информации (мониторов, принтеров, виртуальных шлемов и т.д.).

Обобщая изложенное, можно сказать, что каждый уровень служит неким буфером, преобразующим свойства (ограничения, требования) верхнего уровня в свои и свойства (ограничения, требования) нижнего уровня.

Проиллюстрируем взаимодействие уровней в ИС, обладающей целостностью (1), (2). Без нарушения общности для упрощения примера предположим, что:

- Все характеристики уровней ИС φ^{Y} постоянны во времени. ИС функционирует на промежутке $T = [t_1; t_2] = 1$ месяц.
- Показатель эффективности применения ИС $I^{ИС}$ оценивается количеством целевых задач, решённых ИС за требуемое время ($T = 1$ месяц).
- Все решаемые ИС задачи одинаковы.
- Для проведения расчётов учтём, что $Q^{Y} = X^{Y} \times T$, где X^{Y} – множество требуемых пространственных состояний уровня, и преобразуем (2) следующим образом:

$$\int_{t_1}^{t_2} \int_{X^{П}} \int_{X^{АО}} \int_{X^{ПО}} \varphi^{ИС}(x^{ИС}) dx^{ПО} dx^{АО} dx^{П} dt = T * \int_{X^{П}} \int_{X^{АО}} \int_{X^{ПО}} \varphi^{ИС}(x^{ИС}) dx^{ПО} dx^{АО} dx^{П} = I^{ИС}. \quad (4)$$

- Все компоненты векторов состояний уровней оцениваются двоично: 1 – компонент работоспособен, 0 – компонент неработоспособен. В этом случае состояние уровня ИС будет описываться двоичным числом, где каждому разряду соответствует свой компонент. В этом случае можно сказать, что задано компактное дискретное метрическое пространство, образованное дискретной метрикой $\eta(x_i, x_j) = \begin{cases} 0, x_i = x_j \\ 1, x_i \neq x_j \end{cases}$. Потенциал поля эффективности $\varphi^{ИС}$, заданный на этом пространстве, будет непрерывной функцией.
- Предположим, что $\varphi^{ИС}(x^{ИС}) = 1 + \frac{1}{1 + x^{ПО}}$, подставим $\varphi^{ИС}(x^{ИС})$ в (4):

$$T * \int_{X^{П}} \int_{X^{АО}} \int_{X^{ПО}} (1 + \frac{1}{1 + x^{ПО}}) dx^{ПО} dx^{АО} dx^{П} = T * x^{П} * x^{АО} * (\log(1 + x^{ПО}) + x^{ПО}) = I^{ИС}. \quad (5),$$

где $x^{П}$, $x^{АО}$, $x^{ПО}$ – характеристики объёмов в конкретных состояниях из множеств $X^{П}$, $X^{АО}$, $X^{ПО}$.

- Все уровни ИС имеют 3 элемента, т.е. состояния уровней описываются двоичным числом, содержащим 3 разряда, следующим образом.

Уровень ПО

Средство криптографической защиты информации (СКЗИ) – первый разряд $x'^{ПО}_1$, операционная система (ОС) – второй разряд $x'^{ПО}_2$, прикладная подсистема (ПрП) – третий разряд $x'^{ПО}_3$. При этом $x'^{ПО}_3 \cup x'^{ПО}_2 \cup x'^{ПО}_1 = x^{ПО}_{<3>}$.

Пример. Для записи 001 – СКЗИ работоспособно, ОС неработоспособна, ПрП – неработоспособна.

Пример. Для записи 011 – СКЗИ работоспособно, ОС работоспособна, ПрП – неработоспособна.

Возможно 8 состояний уровня. Зададим ППЭ таблично.

Состояние уровня ПО $x^{ПО}_{<3>}$	000	001	010	011	100	101	110	111
Значение характеристики объёма $x^{ПО}$ в состоянии	0	0	0	2	0	0	5	10

Уровень АО

Монитор – первый разряд $x'^{АО}_1$, манипулятор «мышь» – второй разряд $x'^{АО}_2$, клавиатура и системный блок – третий разряд $x'^{АО}_3$. При этом $x'^{АО}_3 \cup x'^{АО}_2 \cup x'^{АО}_1 = x^{АО}_{<3>}$.

Возможно 8 состояний уровня. Зададим ППЭ таблично.

Состояние уровня АО $x^{АО}_{<3>}$	000	001	010	011	100	101	110	111
Значение характеристики объёма $x^{АО}$ в состоянии	0	0	0	0	0	3	0	10

Уровень П

Системный администратор – первый разряд $x'^{П}_{1}$, рядовой сотрудник – второй разряд $x'^{П}_{2}$, начальник – третий разряд $x'^{П}_{3}$. При этом $x'^{П}_{3} \cup x'^{П}_{2} \cup x'^{П}_{1} = x_{<3>}^{П}$.

Возможно 8 состояний уровня. Зададим ППЭ таблично.

Состояние уровня П $x_{<3>}^{П}$	000	001	010	011	100	101	110	111
Значение характеристики объёма $x^{П}$ в состоянии	0	0	5	7	6	9	8	10

Множество всех возможных пространственных состояний ИС получается путём объединения пространственных состояний уровней $X_{<9>}^{ИС} = x_{<3>}^{П} \cup x_{<3>}^{АО} \cup x_{<3>}^{ПО}$, т.е. общее состояние ИС будет описываться 9-разрядным двоичным числом. Всего возможно $2^9 = 512$ состояний.

Предположим, что ИС решает задачи по организации гос. закупок в электронном виде. По требованиям нормативно-правовой составляющей разрешается использовать только юридически значимые документы, т.е. использование СКЗИ обязательно [5, 6] (значит, вектор $x_{<3>}^{ПО}$ не может принимать значения из множества {000, 100, 010, 110}). На обеспечение гос. закупок выделено N у.е. (требование экономической составляющей обеспечивающего уровня). В ИС разрешается использовать не более 1 человека (вектор $x_{<3>}^{П}$ может принимать значения из множества {000, 001, 010, 100}). На своём промежутке функционирования T необходимо решить 800 одинаковых задач. *Верхний уровень влияет на нижний уровень путём формирования множества X нижнего уровня.*

С вышеназванными требованиями обеспечивающего уровня ИС может решить максимум 660 задач. Однако в этом случае $I^{ИС} < I^{Треб}$. Достичь требуемого значения показателя эффективности можно, например, скорректировав требования обеспечивающего уровня по комплектации ИС персоналом (*нижние уровни влияют на верхние через показатель эффективности применения (3)*). Двух человек достаточно для того, что бы обеспечить $I^{ИС} \geq I^{Треб}$. Состояние $x_{<3>}^{П} = <111>$ избыточно.

Оценивая стоимость применения каждого элемента ИС, возможно создать ИС, удовлетворяющую требованиям, экономической составляющей обеспечивающего уровня.

Рассмотрим, как целостность (1), (2) влияет на безопасность ИС. Здесь важно помнить, что основная задача злоумышленника состоит в том, чтобы заставить атакуемую систему работать в своих интересах [1], т.е. сформировать $\Delta I^{ИС}$ либо $\Delta Q^{ИС}$.

Аксиома. Злоумышленник может влиять только на φ^{Y} либо Q^{Y}.

Ограничение 1. Любые изменения Q^{Y} влекут изменение φ^{Y} и φ нижних уровней.

Атакуя в пределах одного уровня, злоумышленник может корректировать только производительность атакуемого уровня ИС (φ^{Y}). Если уровень обладает целостностью (1), то изменение пространства требуемых состояний уровня средствами самого уровня невозможно, так как это пространство формируется вышестоящими уровнями (метасистемой) на этапе создания уровня.

Ограничение 2. Изменение Q^{Y} возможно только средствами верхнего уровня.

Изменение производительности уровня отражается на всех вышестоящих уровнях, поскольку изменяется показатель эффективности применения уровня (см. выражение (3))

$$\int_{Q^{Y}} \Delta\varphi^{Y}(r^{Y}) dr^{Y} \Rightarrow \Delta I^{Y}. \qquad (6).$$

Как следует из выражения (6), аксиомы и ограничения 1, обнаружить воздействие злоумышленника в ИС, обладающей целостностью, можно по ΔI^{Y}. Задача защиты сведётся к подбору такого $\Delta Q^{ИС}$, чтобы $\Delta I^{ИС} \to 0$. Более подробно взаимодействие злоумышленника и информационной системы в рамках одного уровня рассмотрено в [7].

Если уровень атакуется средствами вышестоящих уровней, то злоумышленник может воздействовать как на пространство требуемых состояний атакуемого нижнего уровня (Q^{Y}), так и на его производительность (φ^{Y}). Тогда задача злоумышленника сводится к тому, чтобы подобрать такие изменения Q^{Y} и φ^{Y}, чтобы I^{Y} достиг требуемого злоумышленнику значения либо остался неизменным, т.е.

$$\Delta Q^{Y}, \Delta\varphi^{Y} : (I^{Y} \rightarrow I^{\text{треб. зл.}} \text{ или } \Delta I^{Y} \rightarrow 0).$$

В случае с неизменным I^{Y} атака не будет обнаружена. Однако стоит отметить, что изменение Q^{Y} какого-то уровня возможно только путём изменения Q^{Y+1} верхнего уровня (ограничение 2), что вызовет $\Delta\varphi^{Y+1}$, а затем ΔI^{Y+1}. А изменение Q^{Y+1} потребует изменения Q^{Y+2} и т.д. Следовательно, если в ИС *все* уровни обладают целостностью, то проведение атаки становится невозможным (при наличии необходимых ресурсов). Либо злоумышленник должен подняться вверх до такого уровня, где целостность не проверяется, а это, согласно теореме Гёделя о неполноте [2], вполне возможно. Очевидно, чем выше уровень, на который воздействует злоумышленник, тем больше возможностей по корректировке $Q^{\text{ИС}}$ он имеет. Противостоять этому возможно только путём контроля целостности каждого уровня ИС и целостности связей между уровнями (выражения (1), (2) и (3)). Названные выражения *формализуют* базовую закономерность – *целостность информационной системы* – и позволяют, применяя готовые математические аппараты, изучать свойства информационной системы.

Таким образом, предложенная в статье модель ИС формализует связь между пространственно-временными состояниями ИС и эффективностью применения ИС, позволяет выбрать из множества возможных пространственно временных состояний требуемые состояния, т.е. те, что позволят достичь требуемого значения показателя эффективности применения ИС. В статье также кратко продемонстрировано, как выглядят вопросы обеспечения безопасности в ИС, обладающей целостностью.

Для практического применения модели необходимо разработать метод формализации состояний ИС и метод, формализующий зависимость структуры ИС и функций ИС.

Литература

1. Расторгуев С.П. Информационная война. – М. : Радио и связь, 1998. – 416 с.

2. Успенский В.А. Теорема Геделя о неполноте. – М. : Наука, 1982. – 111 с.

3. Бурлов В.Г. Синтез модели вычислений в условиях разрушаемой программно-аппаратной среды // Сборник алгоритмов и типовых задач. – 2002. – №20. – С. 220–235.

4. Бурлов В.Г. Основы моделирования социально-экономических и политических процессов (Методология. Методы). – СПб. : Стратегия будущего, 2007. – 267 с.

5. Приказ ФСБ России от 9 февраля 2005 г. №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» // Российская газета от 19 марта 2005 г. №55.

6. Федеральный закон от 10 января 2002 года №1-ФЗ «Об электронной цифровой подписи» // Российская газета от 12 января 2002 г. №6.

7. Грызунов В.В. Структурно-функциональный синтез модели системы предотвращения вторжений // Проблемы информационной безопасности. Компьютерные системы. – 2006. – №2. – С. 31–38.

Грызунов Виталий Владимирович
Канд. техн. наук, преподаватель кафедры вычислительной техники
Военно-космической академии им. А.Ф. Можайского, г. Санкт-Петербург
Эл. почта: viv@nwudc.ru
Тел. +7 (812) 955-6933

V.V. Gryzunov

The analytical model of the whole information system

The analytical model of the whole information system has been represented and commented. The problems of the security of information in the whole information systems are shown to be non-topical.

Keywords: the information protection, security of the information system, the model of the information system, wholeness, the interaction of levels of the information system.