ЭТАЛОННАЯ МОДЕЛЬ ОБЪЕКТА АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

THE REFERENCE MODEL OF THE OBJECT OF SECURITY AUDIT

V. Voevodin

Summary. it is reported about the relevance of the information security audit when making a decision to ensure the protection of information. The model of a problem situation is given, its philosophical description is given. The General statement of the problem of information security audit, the use of forces and means of audit is carried out, the concept of a channel for monitoring individual properties is introduced, the results achieved and the directions of further research will be reported.

Keywords: audit, information security, model of the object of audit, audit certificates, audit evidence, monitoring channel.

Воеводин Владислав Александрович
К.т.н., доцент, Национальный исследовательский университет «МИЭТ»
vva541@mail.ru

Аннотация. Сообщается об актуальности аудита информационной безопасности при принятии решения по обеспечению защиты информации. Приводится модель проблемной ситуации, дается её философское описание. Осуществляется общая постановка задачи аудита информационной безопасности, применения сил и средств аудита, вводится понятие канала наблюдения за отдельными свойствами, сообщатся о достигнутых результатах и направлениях дальнейших исследований.

Ключевые слова: аудит, информационная безопасность, модель объекта аудита, аудиторские свидетельства, аудиторские доказательства, канал наблюдения.

Актуальность темы публикации вытекает из результатов анализа общего содержания задачи аудита информационной безопасности (АИБ), его места в обеспечении принятия решений по обеспечению защиты информации.

Задача АИБ существует и имеет практический смысл постольку, поскольку существует проблема выбора рационального решения по обеспечению информационной безопасности (ИБ). Это определяет роль и место АИБ в управлении ИБ, как средства, снижающего информационную неопределенность при принятии решения. Влияние информационной неопределенности на эффективность принимаемых решений исследованы в [13, 14, 15].

Органы управления перед принятием управленческого решения стремятся снизить информационную неопределённость, для этого готовы пожертвовать частью выделенного ресурса в обмен на обоснованность принимаемого решения.

В общем случае принятие решения можно определить, как преобразование информации о состоянии объекта управления в количественные или качественные составляющие информации управления. Такая концепция является наиболее приемлемой для обоснования актуальности аудита, в том числе аудита ИБ, в результате которого добывается информация о состоянии объекта управления и окружающей среде, являющихся базой для принятия управленческого решения.

По своей сути задача распределения ресурса между аудитом и непосредственной реализацией принятого решения является противоречивой, если принимать решение в условиях полной информационной неопределенности, аудит не проводить, то вероятность принятия рационального решения будет очень малой, с другой стороны — весь ресурс сосредоточить на аудите, тогда времени на реализацию принятого решения практически не остается. В той ситуации актуальной является гипотеза о существовании, так называемой, «золотой средины». Как её отыскать?

Модель проблемной ситуации

Суть проблемной ситуации заключается в том, что для организации аудита необходимы знания: а) об эталоне объекта аудита; б) модель реального объекта аудита, в результате сравнения которых выводится соответствующее аудиторское заключение. На практике эталонная модель ОА задается в виде требований заказчиков аудита, которыми могут выступать регулятор в той или иной области деятельности, партнёры, потребители услуг аудируемой организации, страховые компании, правоохранительные органы.

Таким образом, эталонная модель объекта аудита (ЭМОА) *— документ, в котором определены требования* (эталон) *защиты информации того или иного ОА — например,* требований стандарта Банка России СТО БР ИББС-1.0–2014; требований ISO/IEC27001; **требований договора; требований по защите информации**

вновь создаваемой и внедряемой информационной системы; требования стандартов по управлению качеством продукции серии ISO 9000/10000; **стандарт** оценки уровня зрелости организации по управлению проектами — PMBOK; пороговый уровень риска информационной безопасности — RПор.; требования по обеспечению защиты информации в критических информационных инфраструктурах и др.

Эталонная модель ОА является внешним дополнением, которое необходимо для того чтобы обеспечить полному и не противоречивость аудиторского заключения. Роль внешнего дополнения в обеспечении полноты и непротиворечивости исследована Гёделем, основные положения теоремы приведены в [12, 7]. Важным условием является, то, что и аудитор, и Заказчик аудита согласны с этими требованиями (внешним дополнением) и документально зафиксировали свою позицию.

Другими словами, требуется модель эталона — YTр. с которой будет сравниваться реальная модель того или иного объекта аудита, полученная в результате аудита,— Y(π). Реальная модель ОА строится (создается) в процессе аудита и зависит от полноты программы аудита (концептуальной модели ОА) и эффективности плана применения сил и средств аудита — π, выделенных для его проведения.

Причем важно пронимать, что эталонная модель ОА инвариантна для любой прикладной области и имеет прикладную особенность лишь при построении множества каналов изменения (наблюдения) — O={oi}, где i — индекс соответствующего канала измерения того или иного свойства ОА.

Для понимания сути проблемы аудита следует мысленно встать на философские позиции и увидеть две категории: а) истинное состояние ОА и б) эмпирическое (опытное) проявление этого состояния в результатах аудиторских наблюдений, на основании которых аудитор выводит суждение об истинном состоянии ОА. Истинное состояние аудитор желает познать посредством количественных и качественных наблюдений за свойствами (характеристиками) данного объекта, и оно, для аудитора, является идеальным (неизвестным). Истинное состояние объекта аудита не зависит ни от средств наблюдения, ни от познаний самого аудитора и является для него абсолютной истиной, которую он желает познать.

Результаты аудиторских наблюдений, напротив, являются продуктами познания объекта аудита, представляя собой лишь оценки наблюдаемых свойств, добытые посредством наблюдения, они зависят не только от самого аудитора, но еще и от применяемых методов и средств наблюдения, от технических средств, с помощью которых проводятся наблюдение, и от методов обработки результатов аудиторских наблюдений.

Разница между результатами измерений, полученных при наблюдении за тем или иным свойством ОА и его истинным значением измеряемой (наблюдаемой) величины характеризует погрешность наблюдения (измерения), что определяет аудиторский риск.

Процесс АИБ, независимо от того на каком методологическом уровне исследования (проблемный, концептуальный, операциональный, детальный) он рассматривается, может быть представлен в виде двух, реализуемых последовательно, этапов:

1. Подготовительный — решается задача анализа, от общего к частному — от требования (эталона) к распределению сил и средств АИБ по задачам и времени — плану применения.
2. Непосредственное применение сил и средств АИБ — решается задача синтеза, от частного к общему — от добытых аудиторских свидетельств (АС), к аудиторским доказательствам (АД), а от них к аудиторскому заключению (АЗ).

Краткое содержание этапов:

1. Задачи анализа — от общего к частному:
- постановка задачи — модель проблемной ситуации, которая служит основанием для разработки концептуальной модели ОА;
- концептуальная модель ОА является основой для разработки программы АИБ — перечень существенных свойств ОА и соответствующих каналов их наблюдения — измерительная модель, которая строится в соответствии с ИСО 27004.
- план применения сил и средств АИБ — распределение ресурса по задачам и времени.

2. Задачи синтеза — от частного к общему:
- в результате реализации плана АИБ добываются аудиторские свидетельства — осуществляются соответствующие измерения существенных свойств ОА;
- результаты измерений служат основанием для вывода, групповых показателей и аудиторского заключения в целом — степень соответствия ОА принятому эталону.
- учитывая, что, чаще на практике, выделенный ресурс для АИБ не покрывает требуемую ресурсоемкость для полного исследования всех свойств ОА, то существует определенный аудиторский риск совершения ошибок первого и второго родов, который характерен для принятого плана АИБ.

Также актуальность темы публикации связана с изменениями правого и нормативного полей, регулиру-

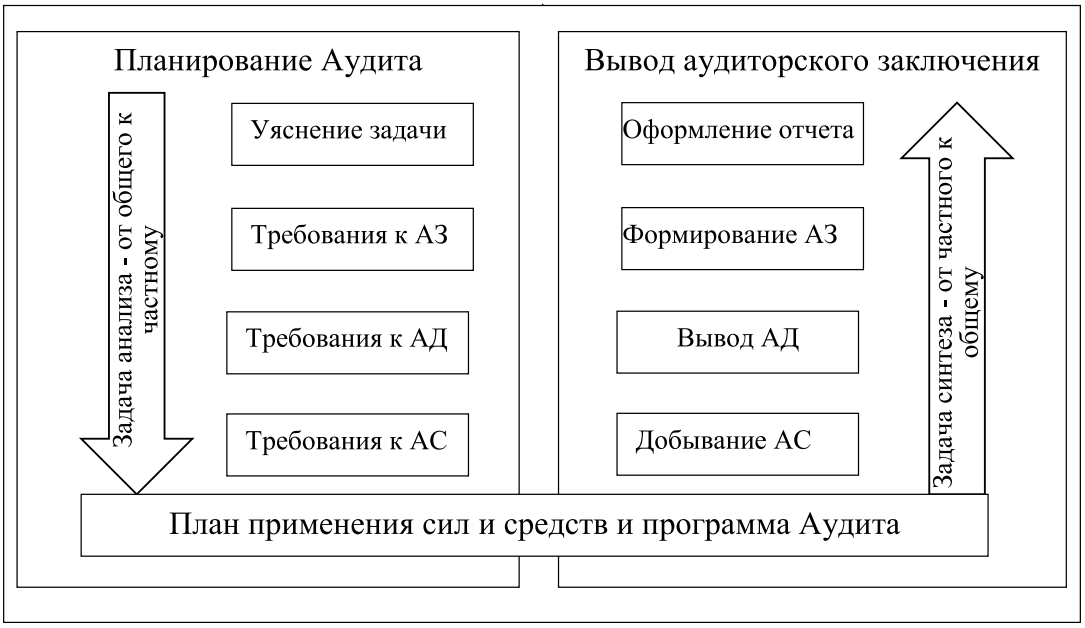

Рис. 2. Иерархическая классификация задач аудита

ющих отношения по обеспечению защиты информации объектов, отнесенных к критической информационной инфраструктуре (КИИ) [8]. Успешное решение задачи АИБ позиционируется как важнейшая задача по обеспечению ИБ, позволяющая снизить информационную неопределённость при принятии решения по обеспечению ИБ и обеспечить, тем самым, повышение эффективности их применения [5].

Для того чтобы обосновать необходимый для аудита ресурс — время, силы и средства, оценить аудиторский риск, существенность наблюдаемых аудиторских свидетельств требуется, наряду с эталонной моделью ОА, адекватная модель реального ОА и самого АИБ как процесса познания ОА.

Для цели настоящей статьи используется классификация моделей, приведенная в [3], а для разработки требований к модели ОА (Модель) и рекомендаций по моделированию — общий подход, приведенный в [3, 7] с учетом индивидуальных особенностей моделируемой предметной области.

По сути задача АИБ состоит в измерении уровня соответствия ОА некоторому, наперед выбранному, эталону (внешнее дополнение) — это может быть стандарт, условия договора, пороговое значение риска ИБ (риск аппетит) и другие требования к ИБ. Задача сводится к вычислению значения, в общем случае, векторного показателя соответствия $W = (W_1, W_2, \ldots, W_n)$, где W_i, $i = 1, 2, \ldots, n$, n — число частных показателей соответствия свойств ОА эталону.

Результатом решения задачи АИБ являются векторные числовые оценки $W(\pi)$, полученные при реализации π -го плана АИБ, принадлежащего множеству допустимых $\pi \in \Pi$, при реализации которых выполняются ограничения на выделенный ресурс — $R(\pi) \leq R_0$, Π — множество допустимых планов АИБ, $R(\pi)$ — ресурс (силы и средства) требуемый для реализации плана АИБ — π, R_0 — ресурс (силы и средства) выделенные для проведения АИБ в целом. Каждая такая оценка $W(\pi)$ характеризует уровень соответствия ОА требованиям выбранного эталона.

На вербальном уровне задача АИБ формулируется следующим образом: для заданных исходных данных характеризующих: а) ОА, его принадлежность к определенному классу систем (информационные системы персональных данных, информационный системы технологических процессов, информационные системы критической инфраструктуры и т.п.); б) производственные возможности сил и средств аудита.

Первая задача — разработать методику (модель), которая бы позволила построить план применения сил и средства АИБ, который бы обеспечивал приемлемый аудиторский риск при минимизации ресурса.

Вторая постановка — при тех же исходных данных найти такой план АИБ, при котором аудиторский риск был бы минимален, а требуемый ресурс не превышал бы выделенного.

Выбор варианта зависит от предпочтений лица, принимающего решение.

Содержание задачи АИБ определяют следующие основные процедуры:

Построение адекватной эталонной модели ОА, характерной для каждой из задач, обозначенных выше: 1. Оценка качества модели ОА и планирование экспериментов с ней;

3. Вычисление значений $W(\pi)$ показателя эффективности плана применения сил и средств АИБ $\pi \in \Pi$ с использованием соответствующей модели ОА.

В общем виде задачу оценивания эффективности плана применения сил и средств аудита ИБ можно представить формальной записью:

$$W(\pi) = \rho\,[(Y(\pi),\ Y_0)]; \qquad (1)$$

$$\Psi : \left\{ Y \,\middle|\, H : \Pi \times \Lambda \xrightarrow{\Theta} Y(\pi) \right\} \xrightarrow{\Theta} W\ , \qquad (2)$$

где $W(\pi)$ — показатель эффективности π-го плана АИБ, Λ множество аудиторских свидетельств, и каналов их наблюдения, формирующих программу АИБ; Y_0 — требуемый результат АИБ; $Y(\pi)$ — результат АИБ, получаемый при реализации π-го плана аудита $\pi \in \Pi$; π — множество существенных свойств ОА связанных с ними каналов наблюдения, важных для получения АЗ с аудиторским риском не ниже заданного $R(\pi) \le R_0$; ρ — функция соответствия реального результата требуемому, H — модель результата АИБ, позволяющая вычислить значения $Y(\pi)$ для каждого плана АИБ $\pi \in \Pi$, Θ — исходные данные, характеризующие проблемную ситуацию — априорные сведения об ОА.

Отображение Ψ в (2) является отображением множества допустимых планов АИБ во множество допустимых значений показателя эффективности W, с учетом (1) и задается с помощью соответствующей модели ОА.

Приведенная формальная запись задачи АИБ задает в наиболее общем виде (2) модель АИБ с оператором выхода W в форме (1). Ни каких ограничений на характер компонент в (2) не накладывает и поэтому может использоваться как общая исходная основа для моделирования АИБ для ОА произвольной природы, назначения и сложности. Главное требование к модели АИБ — её адекватность исследуемому ОА и поставленной задаче АИБ, иначе невозможно получить положительные результаты моделирования, т.е. оценивание эффективности АИБ на неадекватной модели вообще теряет смысл. Модель ОА считается адекватной, если она с достаточной степенью приближения находится на уровне понимания моделируемых операций лицом, принимающим решение (ЛПР) и аудитором и отражает процесс функционирования ОА во внешней среде.

Моделирование аудиторских операций в значительной мере осложняется тем, что наряду с чисто физическими процессами функционирования разнообразных технических подсистем, агрегатов ОА, приходится моделировать поведение людей в различных формах их взаимодействия, что вынуждает обращаться к неформальным методам интуитивного моделирования, экспертного оценивания, анализа, рефлексий и т.д. В научной литературе существует большое разнообразие подходов и классификации моделей и методов моделирования [11, 9].

В качестве исходного тезиса при моделировании ОА было принято то, что аудитор оценивает не все возможные свойства ОА, а лишь определенную выборку, при чем каждое из наблюденных свойств имеет свою ценность (существенность).

Таким образом, для дальнейших исследований ОА был представлен системой соответствующих свойств ОА с назначением соответствующих процедур их измерения. С каждым свойством связано множество его проявлений. При единичном наблюдении показатель имеет одно конкретное проявление. Но аудитору важно оценивать изменение показателя в зависимости от условий наблюдения. Например, как изменяется вероятность успешной атаки на ОА в зависимости от реализуемой угрозы? Или, как оценить величину ущерба в зависимости от той же успешной атаки? В этом случае принимается, что угроза есть варьируемый (управляемый) показатель, а вероятность успешной атаки и ущерб — наблюдаемые показатели, характеризующие ОА. Также в качестве варьируемых показателей в Модели могут выступать время, положение в пространстве, группа и другие или эти показатели в комбинации, причем эти же варьируемые показатели могут выступать и как наблюдаемые свойства.

При исследованиях на первом этапе ОА был формально определен как система (3), представляющая собой множество наблюдаемых свойств — $\{a_i\}$, с каждым из которого связано множество его проявлений — $\{A_i\}$ и множество варьируемых свойств — $\{b_i\}$, с каждым из которого связано множество его изменений — $\{B_i\}$.

$$\text{ОА} = (\{a_i, A_i\}, i \in N_n\}, (\{b_i, B_i\}), i \in N_m\}, \qquad (3)$$

где $N_n = \{1, 2, \ldots, n\}$ — значение индекса наблюдаемого свойства, n — число наблюдаемых свойств; $N_m = \{1, 2, \ldots, m\}$ — значение индекса варьируемого свойства, m — число варьируемых свойств.

Во многих случаях множества $\{A_i\}$ неизвестны и могут быть получены либо опытным путем, либо на основании философских построений.

На втором этапе исследований, операционные представления наблюдаемых свойств позиционировались как переменные, а операционное представление варьируемых свойств — как параметры. При этом сущность и содержание терминов переменная и параметр приняты в понимании их в классической математике [4].

На отдельных множествах состояния переменных и (или) параметрических множествах могут быть определены математические отношения (шкала) [1], например — отношения порядка или расстояния. Так, например, каждое из наблюдаемых свойств (индекс свойства — переменная) можно ранжировать отношением порядка в зависимости от информативности (параметр) и учитывать эти знания при планировании аудита и оценке аудиторского риска. Формальных выражений для поиска такого соответствия на настоящий момент не получено, поэтому применили экспертные методы. Фундаментальные различия наблюдаемых и варьируемых свойств по аналогии [3] позиционировали как методологические различия, которые по сути и содержанию будут рассмотрены в другой публикации.

На следующем этапе исследования ввели понятия абстрактной и конкретной переменных и параметров. Множество состояний переменной должно отображаться изоморфно (один в один с сохранением всех математических отношений, определенных на нем) в элементы множества состояний конкретной переменной. Изоморфное отображение абстрактной переменной или параметра в элементы конкретной переменной или параметра позиционировалось как конкретизация, обратное преобразование — абстрагирование.

Далее в Модель был введен новый элемент — канал наблюдения [2], под которым понимается операция, вводящая конкретную переменную как образ того или иного наблюдаемого свойства ОА. Канал наблюдения был реализован с помощью функции (4)

$$o_{i:}\, A_i \rightarrow V_{i,} \qquad (4)$$

Считается, что эта функция гомоморфна относительно предполагаемых свойств мужеств A_i и $V_{i,}$ где V_i — множество возможных значений переменной.

Аналогичная функция (5) задает представление варьируемых параметров

$$o_{i:}\, B_i \rightarrow W_{i,} \qquad (5)$$

Концептуальная модель АИБ

KM = {**AC**={ac*i*}}, *i = 1,…, M, где M — число свойств ОА, которое может быть потенциально оценено с помощью доступных процедур и средств измерения.*

Операциональная модель ОА

OM = {AC = {ac$_i$, O$_i$ = {o_{ij}}}}, *i = 1,…, N, N — число существенных свойств ОА, которое вошло в сценарий АИБ, j= 1,…, m$_i$, — индекс канала наблюдения i-го свойства, m$_i$ — число каналов наблюдения i -го свойства ОА. С помощью операциональный модели формируется множество свойств ОА, которое потенциально может быть исследовано при реализации разработанного* **сценария** *АИБ.*

Модель применения сил и средств АИБ

П*M* (π) = {AC (π)={ac$_i$, O$_i$ ={o_{ij}}}}, *i = 1,…, N, N — число существенных свойств, которое вошло в* π *— й план АИБ, j= 1,…, m$_i$, — индекс канала наблюдения i-го свойства, m$_i$ — число каналов наблюдения i -го свойства ОА. С помощью операциональный модели формируется множество свойств ОА, которое будет исследовано при реализации* π *— го плана АИБ. Плановая модель должна обеспечивать оценку эффективности выбранного плана АИБ. Каждый канал наблюдения характеризуется ресурсом, требуемым для его осуществления — требуемые силы и средства АИБ. Требуемые силы рассчитываются по методикам нормирования труда, средства на основании технологических и технических норм. Нормы труда оцениваются затратами на оплату труда с учетом всех действующих налогов. Нормы владения средствами измерений и программными средствами — стоимостью их амортизации и действующими налогами на имущество.*

В настоящее время усилия по исследованию сосредоточены на моделировании нечёткого канала наблюдения [9], а также на разработке теоретических основ АИБ в виде алгебры свойств ОА в которой результаты аудиторских наблюдений позиционируются как аксиомы, а для вывода аудиторских доказательств используются теоремы — предмет следующих публикаций по теме.

Разработанная модель была апробирована в ходе деловой игры по учебной дисциплине «Аудит информационной безопасности», разрабатываются соответствующие ситуационные задачи. Идея моделирования ОА докладывались на профильных конференциях.

Материалы публикации подготовлены с использованием гранта Благотворительного фонда Владимира Потанина.

ЛИТЕРАТУРА

1. Анфилатов В. С., Емельянов А. А., Кукушкин А. А. Системный анализ в управлении.— М. Финансы и статистика, 2002.— 368 с
2. ГОСТ Р ИСО/МЭК 27004–2012. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения — Введ. 2011–01–12 № 681-ст.— М.: Стандартинформ, 2012.— 55 с.
3. Клир Дж. Системология. Автоматизация решения системных задач.— М.: Радио и связь, 1990.— 544 с.
4. Математический энциклопедический словарь / Ю. В. Прохоров.— М.: Научное издательство «Большая Российская энциклопедия», 1995.— 847 с.
5. Материалы VI Конференции «Информационная безопасность АСУ ТП КВО» [Электронный ресурс]: публикации в СМИ,— Режим доступа: http://www.иб-кво.рф/publikatsii, свободный.
6. Надежность и эффективность в технике: Справочник: Т. 3 Эффективность технических систем. /Под общ. Редакцией В. Ф. Уткина, Ю. В. Крючкова. М.: Машиностроение, 1988–328 с.
7. Надежность и эффективность в технике: Справочник: В 10 томах. Т. 3. Эффективность технических систем/ Под общ. Ред. В. Ф. Уткина, Ю. В. Крючкова.— 328 с.
8. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации: [утв. Президентом Российской Федерации Д. Медведевым 3 февраля 2012 г. № 803. Режим доступа: http://www.scrf.gov.ru/security/information/document113/.
9. Пегат А. Нечеткое моделирование и управление / пер. с англ.— М.: БИНОМ. Лаборатория знаний, 2009.— 798 с.
10. Советов Б. Я., Яковлев С. А. Моделирование систем. М.: Высшая школа, 1985.— 271 с.
11. Уемов А. И. Логические основы метода моделирования. М.: Мысль, 1971.— 311 с.
12. Нагель Эрнест, Ньюмен Джеймс Рой. Теорема Гёделя: Пер. с англ. Изд. 2-е, испр.— М.: КРАСАНД, 2010.—120 с.
13. Эшби У. Р. Введение в кибернетику.— М.: ИЛ, 1959.— 432 с.
14. Королев О. Л., Куссый М. Ю., Сигал А. В. Применение энтропии при моделировании процессов принятия решений в экономике.— Симферополь.: «ОДЖАКЪ, 2013.— 147 с.
15. Трухаев Р. Модели принятия решений в условиях неопределенности. М.: Наука, 1981.— 258 с.

Журнал «Современная наука: актуальные проблемы теории и практики»

Национальный исследовательский университет «МИЭТ»