Вестник Сыктывкарского университета.
Серия 1: Математика. Механика. Информатика.
Выпуск 4 (29). 2018

УДК 378.147

МОДЕЛЬ ОБЪЕКТА АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В. А. Воеводин, А. С. Заболотный, Э. О. Настинов

Сообщается об актуальности аудита информационной безопасности при решении задачи защиты информации. Приводятся модели проблемной ситуации, дается её философское описание, формальная модель объекта аудита. Осуществляется общая постановка задачи оценивания эффективности применения выделенных сил и средств, вводится понятие канала наблюдения, сообщается о достигнутых результатах исследований и перспективном направлении исследования.
Ключевые слова: аудит, информационная безопасность, модель объекта аудита, аудиторские свидетельства, канал наблюдения.

Актуальность темы публикации вытекает из анализа общего содержания задачи аудита информационной безопасности (АИБ) и содержания отдельных этапов его реализации. 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 соответствующего решения.

Модель проблемной ситуации

Модель эталона, с которым будет сравниваться модель ОА, — официальный документ, в котором определены требования (эталон) не только по обеспечению ИБ, нужно определить степень выполнения этих требований — например требований стандарта Банка России СТО БР

ИББС-1.0-2014; требований ISO/IEC 27001; требований договора; требований по защите информации вновь создаваемой и внедряемой информационной системы; требований стандартов по управлению качеством продукции серии ISO 9000/10000; стандарт оценки уровня зрелости организации по управлению проектами — PMBOK; пороговый уровень риска информационной безопасности — $R_{\text{Пор.}}$; требований к достоверности международной финансовой отчетности; требований по обеспечению защиты информации в критических информационных инфраструктурах и др. Важным условием является, то, что и аудитор, и заказчик аудита согласны с этими требованиями и официально зафиксировали свою позицию. Другими словами, требуется модель эталона — $Y_{\text{Тр.}}$, с которой будет сравниваться модель того или иного объекта аудита $Y(\pi)$. Модель ОА строится (создается) в процессе аудита и зависит от полноты программы аудита (концептуальной модели ОА) и эффективности плана применения сил и средств аудита, выделенных для его проведения, — π. Причем важно, что модель проблемной ситуации инвариантна для любой прикладной области и имеет прикладную особенность лишь при построении множества каналов изменения (наблюдения) — $O = \{o_i\}$, 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, найденные путем наблюдения, они зависят не только от самого аудитора, но еще и от метода наблюдения за соответствующим свойством, от технических средств, с помощью которых проводятся наблюдение, и 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 [2];

• 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 правового и нормативного полей, регулирующих 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 тем самым повысить эффективность 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 моделью эталона адекватная модель объекта аудита (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, заранее выбранному эталону — 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, при реализации которых $\pi \in \Pi$ 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), выделенный 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: 1) ОА, его принадлежность к определенному классу систем (информационные системы персональных данных, информационный системы технологических процессов, информационные системы критической инфраструктуры и т.п.); 2) производственные возможности сил и средств аудита, разработать методику (модель), позволяющую построить план применения сил и средства АИБ, который бы обеспечивал приемлемый аудиторский риск при минимизации ресурса — это первая возможная постановка задачи АИБ. Вторая возможная постановка: при тех же исходных данных должны отыскать такой план АИБ, при котором аудиторский риск был бы минимален, а требуемый ресурс не превышал бы выделенного. Вы-

бор зависит от предпочтений лица, принимающего решение.

Содержание задачи АИБ определяют следующие основные процедуры:

Построение адекватной модели ОА, характерной для каждой из задач, обозначенных выше:

1. Оценка качества модели ОА и планирование экспериментов с ней.

2. 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:

$$W(\pi) = \rho[Y(\pi), Y_0]; \tag{1}$$

$$\Psi : \{Y | H : \Pi \times \Lambda \overset{\Theta}{\to} Y(\pi)\} \overset{\Theta}{\to} W, \tag{2}$$

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 $R(\pi) \leq R_0$, 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). Никаких ограничений на характер компонент в (2) не накладывается и поэтому (2) 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 классификаций 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, причем каждое из наблюдаемых 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 которых связано множество его *проявлений* — $\{A_i\}$, и множество *варьируемых* свойств — $\{b_i\}$, с каждым из которых связано множество его *изменений* — $\{B_i\}$:

$$\mathbf{OA} = (\{a_i, A_i), i \in N_n\},\ (\{b_i, B_i), i \in N_m\}, \tag{3}$$

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)

$$o_i : A_i \longrightarrow V_i. \tag{4}$$

Считается, что эта функция гомоморфна относительно предполагаемых свойств множеств A_i и V_i, где V_i — множество возможных значений переменной.

Аналогичная функция (5) задает представление варьируемых параметров

$$o_i : B_i \longrightarrow W_i. \tag{5}$$

Концептуальная модель АИБ

$KM = \{A = \{ac_i\}\}$, $i = 1, \ldots, M$, где M — число свойств ОА, которое может быть потенциально оценено с помощью доступных процедур и средств измерения.

Операциональная модель ОА

$OM = \{AC = \{ac_i, O_i = \{o_{ij}\}\}\}$, $i = 1, \ldots, N$, N — число существенных свойств ОА, которое вошло в сценарий АИБ, $j = 1, \ldots, m_i$, — индекс канала наблюдения i-го свойства, m_i — число каналов наблюдения i-го свойства ОА. С помощью операциональной модели формируется множество свойств ОА, которое потенциально может быть исследовано при реализации разработанного сценария АИБ.

Модель применения сил и средств АИБ

ПМ $(\pi) = \{AC(\pi) = ac_i, O_i = \{o_{ij}\}\}\}$, $i = 1, \ldots, N$, N — число существенных свойств, которое вошло в π–й план АИБ, $j = 1, \ldots, m_i$,— индекс канала наблюдения i-го свойства, m_i — число каналов наблюдения i-го свойства ОА. С помощью операциональной 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.

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

Список литературы

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.: Большая Российская энциклопедия, 1995. 847 с.

5. Материалы VI конференции «Информационная безопасность АСУ ТП КВО» [Электронный ресурс]: публикации в СМИ. URL: http://www.ибкво.рф/publikatsii (дата обращения: 10.01.2019).

6. Надежность и эффективность в технике : справочник: в 10 т. Т. 3. Эффективность технических систем / под общ. ред. В. Ф. Уткина, Ю. В. Крючкова. М.: Машиностроение, 1988. 328 с.

7. 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]. URL: http://www.scrf.gov.ru/security/information/document113/ (дата обращения: 10.01.2019).

8. **Пегат А.** Нечеткое моделирование и управление : пер. с англ. М.: БИНОМ. Лаборатория знаний, 2009. 798 с.

9. **Советов Б. Я., Яковлев С. А.** Моделирование систем. М.: Высшая школа, 1985. 271 с.

10. **Уемов А. И.** Логические основы метода моделирования. М.: Мысль, 1971. 311 с.

Summary

Voevodin V. A., Zabolotni A. S., Nastinovn E. O. The object model for audit information security

It is reported about the relevance of information security audit in solving the problem of information security. Models of a problem situation are given, its philosophical description, formal model of object of audit is given. A General statement of the task of evaluating the effectiveness of the allocated forces and funds is carried out, the concept of a monitoring channel is introduced, the results of research and the promising direction of research will be reported.

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

References

1. **Anfilatov V. S., Emelyanov A., Kukushkin A. A.** *Sistemnyy analiz v upravlenii* (System analysis in management), Moscow, Finance and statistics Publ., 2002, 368 p.

2. *GOST R ISO/MEK 27004-2012. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Menedzhment informatsionnoy bezopasnosti. Izmereniya* (GOST R ISO/IEC 27004-2012. Information technology. Methods and means of security. Information security management), Measurements-Enter. 2011-01-12 №681-St. Moscow: Standrtinform Publ., 2012, 55 p.

3. **Clear J.** *Sistemologiya. Avtomatizatsiya resheniya sistemnykh zadach* (Systemology. Automation of solving system problems), Moscow: Radio and communication Publ., 1990, 544 p.

4. *Matematicheskiy entsiklopedicheskiy slovar'* (Mathematical encyclopedic dictionary / Prokhorov), Moscow, Big Russian encyclopedia Publ., 1995, 847 p.

5. Materialy VI Konferentsii «Informatsionnaya bezopasnost' ASU TP KVO» (Proceedings of the VI Conference «information security of APCS»), [Electronic resource]: publications in the media, access Mode: http://www.ибкво.рф/publikatsii, free (date of the application: 10.01.2019).

6. Nadezhnost' i effektivnost' v tekhnike: Spravochnik (Reliability and efficiency in engineering: a Handbook), vol. 3 the Effectiveness of

technical systems, Under. Edition of V. F. Utkin, Y. V. Kryuchkova, Moscow, Mashinostroenie Publ., 1988, 328 p.

7. Osnovnyye napravleniya gosudarstvennoy politiki v oblasti obespecheniya bezopasnosti avtomatizirovannykh sistem upravleniya proizvodstvennymi i tekhnologicheskimi protsessami kriticheski vazhnykh obyektov infrastruktury Rossiyskoy Federatsii: [utv. Prezidentom Rossiyskoy Federatsii D. Medvedevym 3 fevralya 2012 g (The Main directions of the state policy in the field of safety of the automated control systems of production and technological processes of critically important objects of infrastructure of the Russian Federation: [UTV. President of the Russian Federation Dmitry Medvedev February 3, 2012), № 803 mode of access: http://www.scrf.gov.ru/security/information/document113/ (date of the application: 10.01.2019).

8. **Pegat A.** *Nechetkoye modelirovaniye i upravleniye* (Fuzzy modeling and control), translated from English, Moscow, BINOM. Laboratory of knowledge, 2009, 798 p.

9. **Sovetov B. Y., Yakovlev S. A.** *Modelirovaniye sistem* (Modeling of systems), Moscow, Higher school Publ., 1985, 271 p.

10. **Uemov A. I.** *Logicheskiye osnovy metoda modelirovaniya* (Logical foundations of the modeling method), Moscow, Thought Publ., 1971, 311 p.

Для цитирования: Воеводин В. А., Заболотный А. С., Настинов Э. О. Модель объекта аудита информационной безопасности // *Вестник Сыктывкарского университета. Сер. 1: Математика. Механика. Информатика. 2018. Вып. 4 (29). С. 72–82.*

For citation: Voevodin V. A., Zabolotni A. S., Nastinovn E. O. The object model for audit information security, *Bulletin of Syktyvkar University. Series 1: Mathematics. Mechanics. Informatics*, 2018, 4 (29), pp. 72–82.

Национальный исследовательский университет «МИЭТ»

Поступила 10.01.2019