ОСНОВНЫЕ ЭТАПЫ МЕТОДИКИ АУДИТА СИСТЕМЫ МЕНЕДЖМЕНТА БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Найханова Ирина Витальевна

В статье рассматривается методика аудита системы менеджмента безопасности персональных данных. Методика основана на использовании иерархической системы показателей и нечеткого логического вывода по алгоритму Тагаки–Сугено. Компоненты методики обеспечивают возможность адаптации к изменениям внешней среды.

***Ключевые слова**: система менеджмента безопасности персональных данных, алгоритм Тагаки–Сугено, адаптивная модель системы показателей, метод комплексного оценивания системы показателей.*

BASIC STAGES OF AUDIT METHODOLOGY OF PERSONAL DATA SECURITY MANAGEMENT SYSTEM

Irina Naykhanova

The audit methodology of personal data security management system is discussed. The methodology is based on hierarchical indicators system and fuzzy logical output of Takagi–Sugeno algorithm is shown. The components of methodology provide the possibility of adapting to external environment changes are represented.

***Keywords**: personal data security management system, Takagi–Sugeno algorithm, adaptive index system model, method of complex index system evaluation.*

Введение

Целью методики является исследование состояния системы менеджмента безопасности персональных данных (СМБПДн) предприятия на ее соответствие требованиям нормативной базы, которая включает стандарты ГОСТ Р ИСО/МЭК 27001–2006, BS 10012:2009 и законодательную базу в области защиты персональных данных. Методика предназначена для внутреннего и внешнего аудита; по объекту проверки для аудита на адекватность/соответствие; по цели проверки для аудита на соответствие стандартам (комплаенс-аудит) [2].

Аудит на адекватность устанавливает степень соответствия системы документов, представленной организацией по обработке персональных данных, требованиям нормативной базы. Цель аудита адекватности состоит в том, чтобы проверить, что политика, своды правил, руководящие принципы и процедуры отвечают требованиям нормативной базы. Эта часть аудита проводится первой и является кабинетным исследованием и в зависимости от класса информационной системы выполняется либо вне организации, либо в проверяемой организации. Аудит на адекватность может быть проведен как внешними, так и внутренними аудиторами, если они имеют соответствующую квалификацию.

Аудит на соответствие – устанавливает степень понимания, выполнения и соблюдения персоналом документированной системы менеджмента безопасности персональных данных. Аудитор ищет соответствие между запланированными целями и задачами в СМБПДн и их выполнением непосредственно на рабочем месте сотрудника и оценивает:

– в каком порядке, при взаимодействии с кем и посредством каких средств, на основании какой документации, в течение какого времени, и как именно проверяемое подразделение выполняет требование СМБПДн;

– как подразделение, ответственное за безопасность ПДн, документально подтверждает факт пооперационного выполнения установленного порядка;

– как именно исполнители на своем рабочем месте выполняют конкретную процедуру и фиксируют ее фактическое выполнение;

– чем подтверждается качество процесса и его улучшение.

Аудиты на адекватность и на соответствие должны исследовать различные аспекты безопасности персональных данных и найти доказательства их наличия или отсутствия [3].

Критерием оценки результатов аудита на адекватность является только степень документированности, а аудит на соответствие должен оцениваться по трем критериям: степень документированности d_1, степень информированности d_2 и степень выполнения d_3, на основе которых рассчитывается степень соответствия d.

Основные компоненты методики

Методика включает в себя следующие компоненты:

1) адаптивную модель системы показателей;

2) метод комплексного оценивания системы показателей системы менеджмента безопасности персональных данных, который состоит из:

– способа автоматической генерации базы нечетких продукций,

– способов реализации методов получения свидетельств,

– способа реализации алгоритма Тагаки-Сугено.

Адаптивная модель системы показателей. Система показателей [6] построена на основе требований стандартов и законодательства РФ в части защиты ПДн и имеет иерархическую структуру. Иерархия показателей [5] сформирована в виде ориентированного графа G без контуров (дерево). Граф G имеет один корень дерева, в котором находится показатель соответствия СУБПДн требованиям нормативной базы. Построение иерархии заканчивается уровнем листьев, содержащих показатели, для которых можно построить ограниченное линейно-упорядоченное множество принимаемых значений. Остальные вершины распределены среди непересекающихся множеств $G_{1, \dots,} G_m$, и каждое из множеств является деревом, деревья являются поддеревьями корня G.

Граф $G = G_b \cup G_v$, где $G_b = (X_b, R_b)$ – базовая составляющая, X_b – множество вершин, идентифицирующих требования нормативной базы; R_b – множество отношений агрегации типа «is-a» между смежными вершинами (предком и потомком). Граф $G_v = G_{vp} \cup G_{vs}$ – вариативная составляющая, в которой $G_{vp} = (X_{vp}, R_{vp})$, X_{vp} – множество вершин, идентифицирующих процессы проверяемого предприятия, направленные на удовлетворение требований нормативной базы; R_{vp} – множество отношений агрегации типа «is-a» между смежными вершинами; $G_{vs} = (X_{vs}, R_{vs})$, X_{vs} – множество вершин, идентифицирующих свидетельства, полученные в процессе аудита; R_{vp} – множество отношений типа «has a» между смежными вершинами.

Полная иерархия есть $G = G_b \cup G_v$, где $G_v = G_{vp} \cup G_{vs}$, $G_{vs} = G_{vsp} \cup G_{vsd} \cup G_{vso}$, где G_{vsp} – содержит свидетельства, полученные при применении метода наблюдений за процессами; G_{vsd} – содержит свидетельства о качестве документации; G_{vso} – содержит свидетельства о компетенции персонала в области защиты персональных данных.

Таким образом, адаптивная модель системы показателей описывается классической двойкой $M=(X,R)$, где X – множество показателей, R – множество отношений между ними.

Метод комплексного оценивания системы показателей системы менеджмента безопасности персональных данных. Разработанный метод состоит из трех последовательно выполняемых процедур: оценивание свидетельств (нечеткий логический вывод на графе G_{vs}), оценивание процессов СМБПДн предприятия (граф G_{vp}), оценивание общих для всех предприятий процессов СМБПДн (G_b). Процесс оценивания иерархической структуры показателей осуществляется восходящим методом (снизу $\rightarrow$ вверх, слева $\rightarrow$ направо).

Основные этапы методики

Методика аудита системы менеджмента безопасности персональных данных состоит в основном из общепринятых этапов [1, 4, 7]:

1) предварительная подготовка;

2) инициирование и планирование аудита;

3) обследование и сбор информации;

4) анализ полученных данных и выработка рекомендаций;

5) подготовка отчетных документов и сдача работ.

На этапе предварительной подготовки осуществляется создание или корректировка иерархии процессов СМБПДн базовой составляющей и генерация для нее базы знаний.

На этапе *инициирования и планирования процедуры аудита* должны быть определены границы проведения обследования, например:

– комплект организационно-распорядительных документов, подлежащих проверке;

– процессы обработки данных и процессы обеспечения безопасности ПДн, подлежащие проверке;

– структурные подразделения и работники, занимающие обработкой персональных данных, которые будут опрошены.

План аудита способствует тому, чтобы виды деятельности организации, связанные с обработкой персональных данных, проверялись на систематической основе. В план аудита включаются процессы и виды деятельности, которые определены для проверки. В первую очередь должны быть включены технологические процессы обработки персональных данных, которые требуют максимального уровня защищенности и процессы по защите ПДн. Кроме того, определяются проверяемые структурные подразделения, персонал для проведения опроса.

На этом этапе на основе полученной информации должны быть сгенерированы требуемые множества нечетких продукций.

На этапе *обследования и сбора информации* должно быть выполнено обследование выбранных источников свидетельств аудита (документов, процессов обработки персональных данных и их защиты, работников структурных подразделений), и с применением методов получения свидетельств собрана информация.

Этап *анализа полученных данных и выработки рекомендаций* заключается в применении, предложенного в п.3.2 данной главы, метода комплексного оценивания системы показателей. Результаты анализа необходимы для выработки рекомендаций.

Деятельность по этапу «*Подготовка отчетных документов и сдача работ*» является технической, поэтому в данной работе не рассматривается.

В работе предполагается, что каждый аудитор в области обеспечения информационной безопасности ПДн постоянно изучает нормативную базу, касающуюся защиты персональных данных, отслеживает все изменения законодательства. На основе этих знаний аудитор формирует базовую составляющую системы показателей СМБПДн (граф G_b), которую он затем может использовать в процессе проведения аудита.

Рассмотрим более подробно основные этапы методики.

Этап 1. Предварительная подготовка

Работы данного этапа выполняются до начала аудита в период подписания договоров о проведении аудита.

Шаг 1. Анализ нормативной базы в части защиты ПДн.

На этом шаге аудитор изучает законодательство в части защиты персональных данных, стандартов по информационной безопасности на предмет появления новых изменений. Анализирует базовую составляющую на предмет ее оценки на адекватность текущему состоянию стандартов и законодательства.

Шаг 2. Корректировка формализованной нормативной базы.

При изменении нормативной базы аудитор выполняет:

– корректировку базовой составляющей иерархической структуры показателей, граф G_b;

– модификацию базы нечетких продукций R (часть G_b).

Все изменения должны производиться в нечетком логическом контроллере (FLC).

Этап 2. Инициирование и планирование аудита

Шаг 1. Выбор и определение объектов аудита.

На этом шаге должны быть определены границы аудита:

– состав документации по системе менеджмента безопасности персональных данных, подлежащих проверке;

– технологические процессы обработки данных и документация по ним, процессы обеспечения безопасности ПДн, которые подлежат аудиту;

– структурные подразделения предприятия и сотрудники, занимающие обработкой и защитой персональных данных.

По полученной информации формируется план проведения аудита.

Шаг 2. Формирование первой части вариативной составляющей системы показателей (граф G_{vp}).

На данном шаге на основе изучения документации и полученной информации необходимо:

– выявить процессы предприятия, которые приняты для реализации терминальных процессов базовой составляющей системы показателей (базовые терминальные процессы). Эти процессы соответствуют показателям $X_{bt,i} \in G_b$, где $X_{bt,i}$ – листья графа G_b или терминальные вершины. Процессы предприятия будем называть вариативными;

– построить иерархии $G_{vpi,bt}$ вариативных процессов предприятия по $\forall X_{bt,i} \in G_b$, граф $G_{vp} = \bigcup_{i=1}^{l} G_{vp,i}$, где i – текущая терминальная вершина, являющаяся корнем дерева $G_{vp,i}$; l – количество терминальных вершин (листьев) графа G_b;

– ввести в FLC деревья $G_{vp,i}$ и сгенерировать множества нечетких продукций в части G_{vp}.

Шаг 3. Формирование второй части вариатив-

ной составляющей системы показателей (граф G_{vs}).

На данном шаге на основе изучения документации и полученной информации необходимо:

– выявить процедуры, обеспечивающие выполнение вариативных процессов деревьев $G_{vp,i}$. Процедуры определяются для каждого терминального вариативного процесса, которым соответствуют показатели $X_{vpt,i} \in G_{vp}$, находящиеся в листьях дерева $X_{vpt,i}$. По каждой процедуре требуется сформировать:

- множество наблюдаемых процедур $\{X_p\}$;
- множество документов $\{X_d\}$;
- множество опрашиваемых сотрудников $\{X_o\}$;
- определить структурные подразделения, к которым относятся $x_{pj1}, x_{dj2}, x_{oj3}$; ;

– построить иерархии $G_{vsi,vpt}$ процессов организации по $\forall X_{vpt,i} \in G_{vp}$, $G_{vs,i,vpt} = G_{vsi,vpt,d} \cup G_{vsi,vpt,p} \cup G_{vsi,vpt,o}$, граф $G_{vs} = \bigcup_{i=1}^{l} G_{vs,i}$, где i – текущий лист графа G_{vp}, l – количество листьев графа G_{vp};

– ввести в FLC граф G_{vs} и сгенерировать множество нечетких продукций в части деревьев $G_{vs,i}$.

Этап 3. Сбор данных

Шаг 1. Сбор свидетельств.

Сбор свидетельств осуществляется по плану по процедурам иерархии, отображенной в $G_{vs,i}$, с применением методов: «Анализ документов», «Наблюдение», «Опрос». Свидетельства фиксируется в соответствующих таблицах 3.1 – 3.5 по каждому наблюдаемому процессу и сотруднику, по всем инцидентам опроса.

Шаг 2. Занесение значений данных в граф G_{vs} FLC.

Данные таблиц 3.1 – 3.5 с оценками аудитора вводятся в FLC, как значения соответствующих терминальных показателей графа G_{vs}.

Этап 4. Анализ данных и комплексное оценивание системы показателей

Шаг 1. Расчет значений групповых показателей.

Расчет начинается с групповых показателей L_i -1 уровня деревьев $G_{vs,i}$. L_i-ый уровень – это уровень листьев (терминальных вершин) деревьев $G_{vs,i}$. Затем рассчитываются групповые показатели L_i -2 уровня деревьев $G_{vs,i}$ и так далее до корня графа G_b. Для этого осуществляется итеративное выполнение нижеследующих процедур.

Процедура 1. Расчет степени документированности

1. По каждому документу частного показателя $X_{vst,ij} \in G_{vs}$ (для сокращения записи обозначим его p_{S2}) в FLC вводятся оценки аудитора показателей документа: α_1(ИД), α_2(ПД), α_j (ОД) из таблиц 3.1 –3.3.

2. По каждому j_2-му документу j_1-му комплекта документов осуществляется нечеткий логический вывод выходного значения показателя (β_{j_1,j_2}) по алгоритму Сугэно.

3. После получения оценок всех документов комплекта $\{\beta_{j_1,j_2} | j_1 = \overline{1,q_1}, j_2 = \overline{1,q_2}$, где q_1 – количество комплектов документов, q_2 – количество документов в комплекте} выполняется оценка β_{j_1} комплекта документов.

4. По алгоритму Сугэно осуществляется нечеткий логический вывод значения степени документированности d_2 показателя $X_{vst,ij}$.

Процедура 2. Расчет степени выполнения

1. По каждой j-ой процедуре показателя $X_{vst,ij} \in G_{vs}$ в FLC вводятся оценки аудитора.

2. Осуществляется нечеткий логический вывод по алгоритму Тагаки-Сугэно значения степени выполнения d_1 по указанному показателю.

Процедура 3. Расчет степени компетентности персонала – расчет степени компетентности персонала d_3 выполняется аналогично расчету степени выполнения.

Процедура 4. Расчет степени соответствия – степень соответствия d рассчитывается по алгоритму Тагаки-Сугэно, входными лингвистическими переменными являются d_1, d_2 и d_3.

Шаг 2. Расчет значений показателей графов G_{vp} и G_b.

Расчет значений показателей выполняется по каждой их группировке. Для каждой группировки уровня L_i-2 и выше входом являются три лингвистические переменные d_1, d_2 и d_3 смежных вершин-потомков. Результатом применения к ним алгоритма Тагаки-Сугэно являются d_1, d_2, d_3 и d.

Группировки просматриваются слева-направо, снизу-вверх. Последняя группировка – это группировка корневой вершины графа G_b с показателем $x_{b,0} \in G_b$. Этот показатель имеет искомые значения критериев d_1, d_2, d_3 и d.

Этап 5. Подготовка отчетов и рекомендаций

Шаг 1. Анализ полученных значений в нечетком логическом контроллере.

В базе данных FLC сохраняются значения всех показателей, это дает возможность проанализировать каждый процесс, соответствующий показателю: насколько он документирован (анализ иерархии показателей d_2), как выполняется (анализ иерархии показателей d_1) и какова компетентность сотрудников (анализ иерархии показателей d_3) предприятия по конкретному процессу. Для

этого необходимо сформировать в FLC различные сортировки процессов по значениям критериев d_1, d_2, d_3 и d. Это позволит выявить узкие места в СМБПДн.

Шаг 2. Формирование отчета и рекомендаций.

Сохраненные в базе данных значения d_1, d_2, d_3, d позволяют выполнить их классификацию, что обеспечивает возможность сформировать достаточно качественный отчет и точные рекомендации по совершенствованию технологических процессов и процессов, связанных с защитой персональных данных.

Заключение

Разработанная методика позволяет значительно упростить процесс проведения аудита и может служить основой для разработки автоматизированной системы для поддержки аудита системы менеджмента безопасности персональных данных. Компоненты методики обеспечивают возможность адаптации к изменениям внешней среды.

Литература:

1. Голованов В. Б., Зефиров С. Л., Курило А. П. Аудит информационной безопасности / под ред. А. П.Курило. М.: БДЦ-Пресс; 2006. 305 с.
2. Дорофеев А. В., Марков А. С. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. № 1(2). С. 67-73
3. Калашников А. О. Управление информационными рисками объектов критической информационной инфраструктуры российской федерации // Вопросы кибербезопасности. 2014. № 3 (4). С. 35-41.
4. Методы оценки несоответствия средств защиты информации / А. С.Марков, В. Л.Цирлов, А. В.Барабанов; под ред. А. С.Маркова. - М.: Радио и связь, 2012. 192 с.
5. Найханова И. В. Аудит систем менеджмента качества и информационной безопасности // Вестник Московского государственного технического университета им. Н. Э. Баумана. Серия: Приборостроение. 2011. № SPEC. С. 152-156.
6. Найханова И. В. Виды и методики аудита информационной безопасности: состояние и анализ // Информатизация образования и науки. 2012. №3(15). С. 81-94.
7. Найханова И. В. Иерархическая структура показателей аудита безопасности персональных данных // Глобальный научный потенциал. 2014. № 2(35). С. 75-78.
8. Найханова И. В. Разработка системы показателей эффективности системы менеджмента безопасности персональных данных // Труды международного симпозиума "Надежность и качество". 2014. Т. 2. С. 268-270.
9. Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически оправданная безопасность. М.: ДМК Пресс, 2004.384 с.
10. Шелков А. Б., Шульц В. Л., Кульба В. В. Аудит информационной безопасности автоматизированных систем управления // Тренды и управление. 2014. № 4. С. 319-334.
11. France E. Data Protection Audit Manual. 2001. 166 p. URL: http://www.privacylaws.com/Documents/External/data_protection_comp-lete_audit_guide.pdf (дата обращения: 01.12.2014).

References:

1. Golovanov V. B., Zefirov S.L., Kurilo A. P. Audit informatsionnoy bezopasnosti / by ed. A. P.Kurilo, Moscow, BDTs-Press; 2006, 305 p.
2. Dorofeev A. V., Markov A. S. Menedzhment informatsionnoy bezopasnosti: osnovnye kontseptsii, Voprosy kiberbezopasnosti, 2014, N 1(2), pp. 67-73
3. Kalashnikov A. O. Upravlenie informatsionnymi riskami ob"ektov kriticheskoy informatsionnoy infrastruktury rossiyskoy federatsii, Voprosy kiberbezopasnosti, 2014, N 3 (4), pp. 35-41.
4. Metody otsenki nesootvetstviya sredstv zashchity informatsii / A. S.Markov, V. L.Tsirlov, A. V.Barabanov; by ed. A. S.Markov. - M.: Radio i svyaz', 2012, 192 p.
5. Naykhanova I.V. Audit sistem menedzhmenta kachestva i informatsionnoy bezopasnosti, Vestnik Moskovskogo gosudarstvennogo tekhnicheskogo universiteta im. N. E. Baumana. Seriya: Priborostroenie, 2011, N SPEC, pp. 152-156.
6. Naykhanova I. V. Vidy i metodiki audita informatsionnoy bezopasnosti: sostoyanie i analiz, Informatizatsiya obrazovaniya i nauki, 2012, N 3(15), pp. 81-94.
7. Naykhanova I. V. Ierarkhicheskaya struktura pokazateley audita bezopasnosti personal'nykh dannykh, Global'nyy nauchnyy potentsial, 2014, N 2(35), pp. 75-78.
8. Naykhanova I. V. Razrabotka sistemy pokazateley effektivnosti sistemy menedzhmenta bezopasnosti personal'nykh dannykh, Trudy mezhdunarodnogo simpoziuma "Nadezhnost' i kachestvo", 2014, Vol. 2, pp. 268-270.
9. Petrenko S. A., Simonov S. V. Upravlenie informatsionnymi riskami. Ekonomicheski opravdannaya bezopasnost', Moscow, DMK Press, 2004.384 p.
10. Shelkov A. B., Shul'ts V. L., Kul'ba V. V. Audit informatsionnoy bezopasnosti avtomatizirovannykh sistem upravleniya, Trendy i upravlenie, 2014, N 4, pp. 319-334.
11. France E. Data Protection Audit Manual, 2001, 166 p. URL: http://www.privacylaws.com/Documents/External/data_protection_comp-lete_audit_guide.pdf.