Модель подбора состава экспертной комиссии для аудита информационной безопасности объектов критической информационной инфраструктуры

Н. Е. Платов, email: platovne@mail.ru[1]

[1]Краснодарское высшее военное училище
имени генерала армии С.М. Штеменко

Аннотация. *В работе представлен подготовительный этап аудита ИБ: рассмотрены характеристики эксперта как личности и как аудитора, а также требования и рекомендации, применяемые к ним; предложена модель подбора экспертов (членов комиссии) через определение интегрального показателя качеств личности (ИПКЛ) и весового коэффициента.*

Ключевые слова: *Эксперт, аудитор, аудит информационной безопасности, объект критической информационной инфраструктуры, интегральный показатель качеств личности, весовой коэффициент.*

Введение

Какая бы сбалансированная система защиты информации не была бы организована и какие бы эффективные средства защиты информации (криптографические, технические, программные, программно-аппаратные) не были реализованы всегда и везде «слабым звеном» в системе защиты информации будет человек.

И какие бы программно-аппаратные средства оценки защищенности объектов критической информационной инфраструктуры (далее по тексту – КИИ) не применялись – всё равно в комплексе с ними оценку защищенности и соответствия её требованиям нормативных правовых актов РФ (далее по тексту – НПА) в области информационной безопасности (далее по тексту – ИБ) будет проводить и выставлять, в конечном счёте – человек!

В этом контексте оценка защищенности объектов КИИ рассматривается с одной стороны – «кто оценивает», а с другой – «как оценивает».

Анализ НПА показывает, что в современной России ни на государственном уровне, ни в министерствах и ведомствах не установлен однозначный порядок подбора и отбора экспертов в соответствии с требованиями к профессиональным качествам

© Платов Н. Е., 2022

и психологическим характеристикам лиц, занимающихся деятельностью в области аудита ИБ.

На деятельность аудитора влияют как объективные, так и субъективные факторы. Объективные факторы – это общественные отношения, морально-психологический климат, а также уровень развития общества в целом. Субъективные факторы – это, прежде всего, смысл, вкладываемый аудитором в профессиональную деятельность, в свои конкретные поступки и действия, а также знания о средствах, способах, условиях достижения поставленных целей. Адекватное отношение предполагает не только точность восприятия и понимания аудита ИБ, но и верный эмоциональный настрой, отношение к обществу и самому себе [1].

В силу специфики профессиональной деятельности аудиторов, специалисты в данной области должны обладать устойчивостью в настроении, быть невосприимчивыми к давлению системы, иметь способность адекватно реагировать на конфликтные ситуации и со своей стороны не проявлять конфликтности и раздражительности в критических условиях. Психологические особенности личности аудитора должны обеспечивать ему способность принимать меры по предотвращению и урегулированию конфликта интересов, предупреждению коррупции [2].

В связи с этим и требуется выработать модель, которая позволяла бы реализовать эти требования.

Подбор экспертов путем сбора информации о них и вывода весовых коэффициентов экспертов

Положениями пунктов 7.1 «Компетентность персонала» [3] и 7.2.2 «Личные качества» [4] определены требования к аудиторам ИБ.

Рассматриваются две стадии подбора экспертов.

Первая стадия подбора экспертов

Определение ИПКЛ получено в результате симбиоза пункта 7.2.2 «Личные качества» [4] и психологических тестов «КОС», «ФЛО», «ВСК». Путем соотнесения требований указанного ГОСТа к личности аудитора и тестовых факторов была выведена итоговая формула (1) ИПКЛ эксперта с требуемым уровнем морально-нравственного состояния (далее по тексту – МНС) с требуемым количеством стенов – свыше 6.

КОС - психологический тест «Коммуникативных и организаторских склонностей».

ФЛО - психологический тест «16-ти факторный личностный опросник».

ВСК - психологический тест «Волевой самоконтроль».

В соответствии с [4] аудиторы должны обладать необходимыми качествами, обеспечивающими им возможность действовать в соответствии с принципами аудита:

- честность: основа профессионализма;
- беспристрастное представление: обязательство представлять правдивые и точные отчеты;
- должная профессиональная осмотрительность: прилежание и обдуманность решений при проведении аудита;
- конфиденциальность: защита информации;
- независимость: основа беспристрастности аудита и объективности заключений аудита;
- подход, основанный на свидетельстве, рациональный метод достижения надежных и воспроизводимых заключений аудита в систематическом процессе аудита;
- риск-ориентированный подход: подход, учитывающий риски и возможности.

Аудиторы должны проявлять профессиональные качества при выполнении аудита. Желаемое профессиональное поведение предполагает, что аудитор должен быть: этичным, открытым, дипломатичным, наблюдательным, проницательным, гибким, упорным, логичным, уверенным в себе, принципиальным, готовым к совершенствованию, настроенным на сотрудничество.

$$\Psi_{и} = \frac{ВСК + КОС + ФЛО(N) + ФЛО(C) + ФЛО(E) + ФЛО(B) + ФЛО(Q_2) + ФЛО(Q_3) + ФЛО(G)}{9} \quad (1)$$

где: $\Psi_{и}$ – интегральный показатель качеств личности (стены; min=1, max=10; 1-3 – низкий уровень, 4-5 – удовлетворительный, 6-8 – средний, 9-10 – высокий);

ВСК – индексы волевой саморегуляции, настойчивости, самообладания, КОС – индекс коммуникативных и организаторских склонностей, ФЛО(Q2) – самостоятельность / внушаемость, ФЛО(E) – независимость / подчиненность, ФЛО(C) – эмоциональная устойчивость, ФЛО(N) – гибкость / прямолинейность, ФЛО(B) – ограниченное мышление / сообразительность, ФЛО(Q3) – высокий самоконтроль / низкий самоконтроль, ФЛО(G) – выраженная сила «Я» / беспринципность.

После получения ИПКЛ, и в соответствии с критерием свыше 6 стенов, выводится требуемый рейтинг экспертов с устойчивым МНС.

Вторая стадия отбора экспертов

В соответствии с требованиями [3] (п. 7.1 Компетентность персонала) весовой коэффициент эксперта складывается из факторов, перечисленных в табл. 1.

Таблица 1

Весовые значения факторов

Фактор	Вес фактора					
S_1	менее 4 лет	от 4 до 7	от 8 до 11	от 12 до 15	от 16 до 19	20 и более
	0,1	0,2	0,4	0,6	0,8	1
S_2	нет	от 1 до 19	от 20 до 39	от 40 до 59	от 60 до 79	80 и более
	0,1	0,2	0,4	0,6	0,8	1
S_3	нет	к.н.	к.н., доц.	д.н.	д.н., доц.	д.н., проф.
	0,1	0,2	0,4	0,6	0,8	1
S_4	Нет сертификата			Есть сертификат		
	0,5			1		
S_5	нет	1	2	3 и больше		
	0,1	0,3	0,5	1-1/N		
S_6	от 0,05 до 1	от 1 до 2	от 3 до 4	от 5 до 6	от 7 до 8	от 9 до 10
	0,1	0,2	0,4	0,6	0,8	1
S_7	от 0 до 10	от 11 до 28	от 29 до 46	от 47 до 64	от 65 до 82	от 83 до 100
	0,1	0,2	0,4	0,6	0,8	1

Где:

S_1 – трудовая деятельность на должностях подразделений обеспечения безопасности информации и режима секретности (в годах);

S_2 – практика в контрольно-надзорной деятельности (количество проведённых аудитов ИБ);

S_3 – наличие ученой степени / звания;

S_4 – наличие сертификата эксперта как аудитора (да / нет);

S_5 – наличие дипломов / сертификатов / удостоверений о прохождении дополнительного профессионального образования (количество);

S_6 – коэффициент анонимной взаимооценки профессионально-деловых качеств (в баллах);

S_7 – коэффициент компетентности: тестирование независимой специализированной организацией (процент правильно выполненных задач).

Вес фактора содержит показатели, в пределах 6-ти значений от 0,1 до 1, и их критерии, в пределах допустимых значений того или иного фактора.

Каждому эксперту, прошедшего отбор по МНС, присваиваются весовые коэффициенты отдельно по суммарному весу в предметной области и отдельно суммарный вес по всем факторам.

Таблица 2

Суммарные весовые коэффициенты экспертов

Эксперты, i	*Факторы*							$V_{эксп}$, *п/о*	$R_{эксп1}$	$V_{эксп}$, ∑	$R_{эксп2}$
	S_1	S_2	S_3	S_4	S_5	S_6	S_7				
Эксп3	0,2	0,4	0,2	0,1	0,1	0,1	0,8	1,0	5	1,90	5
Эксп2	0,8	0,8	0,2	0,1	0,3	0,2	0,6	1,1	4	3,00	3
Эксп10	0,6	0,4	0,4	1	0,5	0,1	0,6	1,2	3	3,60	2
Эксп7	0,4	0,4	0,1	0,1	0,1	0,4	0,8	1,3	2	2,30	4
Эксп15	0,2	0,1	0,2	0,1	0,1	0,1	0,8	1,0	5	1,60	6
Эксп6	0,6	0,6	0,1	1	0,7	0,1	0,6	1,4	1	3,67	1
					в предметной области						

Значение суммарного весового коэффициента в предметной области ($V_{эксп}$, п/о) учитывается по рангу ($R_{эксп1}$) при назначении эксперта на работу со сбором свидетельств по мерам соответствующего процесса.

Значение суммарного весового коэффициента по всем факторам ($V_{эксп}$, ∑) учитывается по рангу ($R_{эксп2}$) при переназначении эксперта на наиболее загруженные (критичные) работы или работы, требующие немедленного завершения.

Заключение

Одно из ключевых требований к аудитору – его квалификация. Требованиями вышеуказанных ГОСТов установлен принцип регулярного повышения квалификации экспертов и поддержки её на уровне, необходимом для надлежащего исполнения своих должностных обязанностей. Данное требование обоснованно может быть отнесено к аудиторам ИБ. Содержание категории «квалификация аудиторов» должно включать в себя, прежде всего компетентность, под

которой следует понимать способность в практической работе к эффективной и результативной деятельности на основе специальных профессиональных знаний.

Учитываю вышесказанное и применив разработанную модель возможно с большей вероятностью исключить риски, связанные с включением в состав экспертной комиссии должностных лиц с низкими морально-нравственными характеристиками и компетентностью, а также с давлением и навязыванием мнения аудиторам со стороны проверяющей организации, что позволит более полноценно провести аудит ИБ.

Список литературы

1. Степашин С. В. Аудит эффективности как важнейшая форма государственного финансового контроля [Электронный ресурс]. Режим доступа: http://www.ach.gov.ru/ru/chairman/?id=217

2. Кодекс этики и служебного поведения федеральных государственных гражданских служащих аппарата Счетной палаты Российской Федерации (утвержден Приказом Счетной палаты РФ от 08.12.2011 г. № 122) [Электронный ресурс]. – URL: http://www.ach.gov.ru/activities/anticorruption/normative-legal-acts/audit_office/Приказ от 08 12 2011 г № 122 (с измен).pdf (дата обращения 15.12.2021 г.)

3. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27006-2020. Информационные технологии. Методы и средства обеспечения безопасности требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности [Текст]. – Введ. 2021-07-01. – М. Стандартинформ, 2021. – с. 42.

4. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 19011-2021. Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента [Текст]. – Введ. 2021-07-01. – М. Стандартинформ, 2021. – с. 42.