О ПОСТАНОВКЕ ЗАДАЧИ ОЦЕНИВАНИЯ ГОТОВНОСТИ АУДИТОРСКОЙ ГРУППЫ К ПРОВЕДЕНИЮ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ю.А. Ненашева, *магистрант*
В.А. Воеводин, *канд. техн. наук, доцент*
С.А. Калищук, *канд. мед. наук, доцент*
Национальный исследовательский университет «Московский институт электронной техники»
(Россия, г. Москва)

DOI:10.24412/2500-1000-2024-1-4-139-145

Аннотация. *Приводятся результаты исследования требований к компетентности аудиторов и готовности аудиторской группы, существующих методов оценки компетентности аудиторов и готовности аудиторской группы. Исследования проводились в отношении значимых объектов информационной инфраструктуры, функционирующих в условиях воздействия угроз. Результаты исследования показали, что возможности методического обеспечения по оценке готовности аудиторской группы в целом к проведению аудита информационной безопасности недостаточны для объективной оценки компетенции аудиторов и готовности аудиторской группы в целом. Обосновывается необходимость в разработке методики оценки компетенции аудиторов и готовности аудиторской группы к проведению аудита информационной безопасности. Приводится постановка задачи исследования, результаты анализа существующих методов, алгоритм оценивания готовности аудиторской группы.*

Ключевые слова: *аудит, аудит информационной безопасности, аудиторская группа, готовность аудиторской группы, программа аудита.*

Анализируя лучшие практики в области информационной безопасности [1-3], можно утверждать, что перед началом аудита информационной безопасности (АИБ) существует необходимость в обеспечении соответствующей компетенции аудиторов и готовности аудиторской группы (АГ) в целом. Особенно это актуально для аудита объектов подверженных воздействию угроз. Это связанно, прежде всего с тем, что методы оценивания, ориентированные на штатные условия применения объекта аудита основаны на репрезентативной статистике, что для условий воздействия угроз не применимо.

Соответствующий уровень компетенции аудитора достигается путем определения требуемого уровня знаний и навыков, целенаправленным обучением и оценивания уровня его подготовки к проведению практического аудита.

Достоверность и полнота аудиторского заключения в значительной степени зависит от компетенции аудиторов и готовности АГ в целом. Готовность АГ определяется соответствующими компетенциями членов АГ и всеми видами обеспечения: финансовым, кадровым, информационным, правовым, нормативным, методическим обеспечением.

Для подтверждения знаний и умений аудиторов перед началом АИБ следует проводить оценку их компетентности на основании определенных критериев, включая требования к образованию, опыту работы, прохождению повышения квалификации. Требования (критерии) к компетенции задаются в программе аудита исходя из цели, области аудита и особенностей объекта аудита (ОА).

Оценка компетентности проводится посредством изучения личных качеств и способностей применять знания, умения и навыки, и соответствия их специфике решаемых задач. Компетентность каждого аудитора может быть различной. В совокупности компетенции отдельных аудиторов при их организации определяют готовность АГ в целом.

Актуальность исследований определяются тем, что существующие подходы ориентированы на обеспечении компетенции отдельных аудиторов для проведения аудита объектов функционирующих в штатных условиях. Для подготовки и оценивания готовности АГ для проведения аудита объектов, подверженных угрозам с существующие е методы не приспособлены. Прежде всего это связано с тем, что отсутствует какая-либо статистика функционирования объекта в условиях воздействия угроз. Основным методом добывания аудиторских свидетельств является моделирование объекта аудита и процессов его функционирования.

Источники исходных данных для формирования методики. Для лица, управляющего программой аудита определены знания, которыми он должен обладать в соответствующем стандарте [1, 2]:

- принципы, методы и процессы АИБ;
- стандарты на системы менеджмента ИБ и иные нормативные документы;
- сведения о проверяемой организации (такой как: вид деятельности организации; производство товаров и услуг; процессов организации; заинтересованные стороны, их потребности и ожидания);
- нормативные правые акты, требования, применимые к деятельности проверяемой организации;
- вопросы управления рисками, проектами и процессами, а также информационно-коммуникационные технологии,
- результаты экспертного оценивания.

Требования к компетентности руководителя АГ приведены в [1,2]:

- планировать АИБ;
- обеспечить результативное использование ресурсов в ходе АИБ;
- организовать взаимодействие с заказчиком АИБ и с проверяемой организацией;
- руководить подготовкой аудиторов стажеров;
- руководить АГ при проведении АИБ, оперативно реагировать на изменяющуюся обстановку;
- разрешать инциденты и конфликты, возникающие при проведении АИБ;
- организовать подготовку аудиторов и деловое слаживание АГ в целом;
- оценивать уровень компетенции аудиторов и готовность АГ в целом;
- готовить аудиторское заключение и формировать отчет для заказчика.

При формировании АГ и конкретизации требований к компетенции аудиторов АГ могут предъявляться дополнительные требования:

- цель, область, критерии и продолжительность АИБ;
- вид АИБ;
- требования АГ для проведения АИБ;
- требования нормативных правовых актов;
- возможность конфликта интересов с проверяемой организацией;
- возможность членов АГ результативно сотрудничать с проверяемой организацией.

Доверие к АИБ и готовность АГ напрямую зависит от компетентности членов АГ. Для этого члены АГ должны знать [1, 2]:

- принципы, процедуры и методы АИБ, методические приемы добывания объективных аудиторских свидетельств;
- структуру системы управления информационной безопасностью проверяемой организации;
- бизнес-процессы проверяемой организации их уязвимости источники угроз;
- нормативные правовые акты в части касающейся и иметь представление о внутренних документах организации по обеспечению защиты информации.

Поддержание необходимых знаний и навыков аудиторов, руководителей АГ, а также лиц, управляющих ПА должно обеспечиваться соответствующими постоянными мероприятиями по профессиональному развитию в сфере АИБ.

Для этого требуется планировать, реализовывать и документировать оценку компетентности аудиторов в целях проведения результативного АИБ.

Оценка компетентности осуществляется поэтапно [4,5]:

1) начальное оценивание;
2) оценивание аудиторов при отборе в состав АГ;
3) периодическое оценивание компетенции и повышение квалификации;

Оценка компетентности содержит четыре основных этапа:

1) определение требований;

2) выбор соответствующего метода и методики оценивания;

3) проведение оценки.

При начальном оценивании необходимо учитывать:

- размер, вид деятельности и сложность проверяемой организации;
- цель и объем разрабатываемой ПА;
- сложность проверяемой системы менеджмента ИБ;
- методы АИБ;
- роли и обязанности в проведении АИБ;
- неопределенность в достижении целей АИБ;
- требования заказчика АИБ.

Эти исходные данные позволяют определить какими знаниями и умениями должен обладать аудитор в составе АГ для проведения качественного АИБ.

Критерии оценивания, устанавливаемые на втором этапе, задаются в ПА и могут быть количественными или качественными. Количественные – опыт работы, длительность обучения, количество часов подготовки в области АИБ, количество проведенных АИБ и другое. Качественные – личные качества, способность применять знания и умения для решения практических задач АИБ. При отсутствии статистических данных рекомендуется применять методы экспертных оценок, что актуально при подготовке АГ к аудиту объектов, подверженных воздействию угроз [6].

При выборе метода оценки необходимо руководствоваться тем, что должно использоваться не менее двух методов для обеспечения объективного, непротиворечивого, беспристрастного и надежного результата. Выбор метода зависит от конкретной ситуации и от его надежности.

На этапе проведения оценки компетентности аудитора проводится сопоставление информации, собранной об оцениваемом аудиторе с данными, полученными на втором этапе. По результатам оценивания делается вывод о соответствии компетенции аудитора требованиям и возможности его включения в состав АГ. При несоответствии следует направить аудитора на дополнительное обучение.

Из проведённого анализа процесса подготовки и оценки компетентности аудиторов, и возможностей существующего методического обеспечения можно утверждать, что достаточно полно и глубок отработано методическое обеспечение по оцениванию компетентности отдельных аудиторов.

Данное утверждение дополнительно подтверждается и результатами анализа отечественных и международных стандартов [1-3]. Из анализа которых также следует, что положения существующего методического обеспечения, в основном, сосредоточены на оценке знаний, умений и навыков отдельных аудиторов. За рамками методического регулирования остались вопросы, касающиеся оценки готовности АГ и ее делового слаживания.

На практике для оценки компетентности аудиторов зачастую применяются такие методы как анализ записей, обратная связь, интервью, наблюдение, тестирование, анализ после аудита [1, 3].

Анализ записей проводится с целью проверки подготовки аудитора. В качестве записей, подверженных анализу могут быть данные об образовании, опыте в аудиторской деятельности, подготовке, о стаже работы и профессиональной квалификации.

Метод обратной связи позволяет получить информацию о том, как воспринимается работа аудитора заказчиком АИБ, руководителем АГ. Для этого проводятся опросы и анкетирование коллег, работающих с проверяющимся аудитором, сотрудников организаций, которые подвергались проверке со стороны проверяющего аудитора.

Интервью позволяет оценить личные качества и навыки общения аудитора, подтвердить накопленную информацию с прошлой оценки, проверить знания, необходимые для аудиторской деятельности и получить другую дополнительную информацию.

Наблюдение позволяет оценить способности аудитора применять имеющие знания и навыки на практике. Для этого про-

водятся деловые игры, отражающие в полной мере процесс АИБ, в ходе которых можно оценить фактическое качество работы аудитора.

Для оценки теоретических знаний и навыков проверяющего аудитора применяется метод тестирования в виде устных или письменных экзаменов.

Метод – анализ после аудита позволяет получить информацию о действиях аудитора уже в ходе самого АИБ, что дает возможность установить сильные и слабые стороны аудитора, требующие улучшения. После проведенного АИБ можно провести анализ подготовленного аудиторского отчета и при необходимости анализ мнения проверяемой организации.

Преимущества данных методов – это полученные данные о знаниях и навыков об оцениваемых аудиторах, позволяющих сформировать небольшую картину об их деятельности в сфере АИБ. Однако, перечисленные методы не могут быть применены для оценивания готовности АГ в целом.

Приведенные методы выступают в качестве базовых методов оценки компетентности аудиторов, однако эти методы по отдельности и в совокупности не позволяют оценить готовность АГ к практическому аудиту в целом.

Возникает необходимость в подготовке методики оценки готовности АГ к проведению АИБ. Целью разработки методики является обеспечение эффективного управления подготовкой АГ к проведению аудита ИБ.

Постановка задачи. В качестве исходных данных для разработки методики оценки готовности АГ к проведению АИБ выступают:

$\boldsymbol{A} = \{a_i\}$ – команда аудиторов, входящих в оцениваемую аудиторскую группу;

$\boldsymbol{K} = \{k_i\}$ – множество критериев, устанавливаемых для оценивания готовности АГ, определяются в программе аудита;

$\boldsymbol{Z} = \{\boldsymbol{z}_i\}$ – множество задач, поставленных АГ, определяются в ПА;

$\boldsymbol{Ч}$ — момент времени Ч, к которому должна быть готова оценка готовности АГ;

$\boldsymbol{Ч^*}$ — фактический момент времени Ч, к которому планируется получить оценку готовности АГ;

$\boldsymbol{Ч^* < Ч.}$

Необходимо разработать методику, позволяющую для при заданных исходных данных, с учетом заданных временных ограничений, получить достоверную оценку готовности АГ к проведению практического в целом. Выходными данными является $\boldsymbol{M} = \{m_i\}$ – множество метрик, свидетельствующих о готовности АГ.

Результаты исследования применимости существующих методов. Результаты анализа применимости существующих в смежных областях методов оценивания готовности команды для решения тех или иных задач позволяют утверждать, что они могут быть применены в сфере аудита информационной безопасности, требуют адаптации к предметной области. Также исследования показали, что для оценки готовности АГ к совместной работе, состав которой формируется впервые, наиболее эффективным методом будет метод командных ролей Р.М. Белбина. Данный метод позволит оценить возможность АГ выполнять задачи совместно, подобрать хорошо сбалансированную АГ в соответствии с целями ПА, а также определить руководителя АГ. Определение командных ролей данным методом поможет руководителю АГ в дальнейшем грамотно распределять ответственность между членами АГ, сопоставив задачи с возможностями, что способствует качественному проведению АИБ.

Для оценки готовности АГ к проведению АИБ результативным методом может быть метод «Ассессмент-центра», так как данный метод комплексный и состоит из отдельных частных методов, состав и количество которых могут определятся исходя из целей ПА, что позволяет также варьировать и время проведения данной оценки от нескольких часов до нескольких дней. Эффективность данного метода подтверждают статистические данные на рисунке 1.

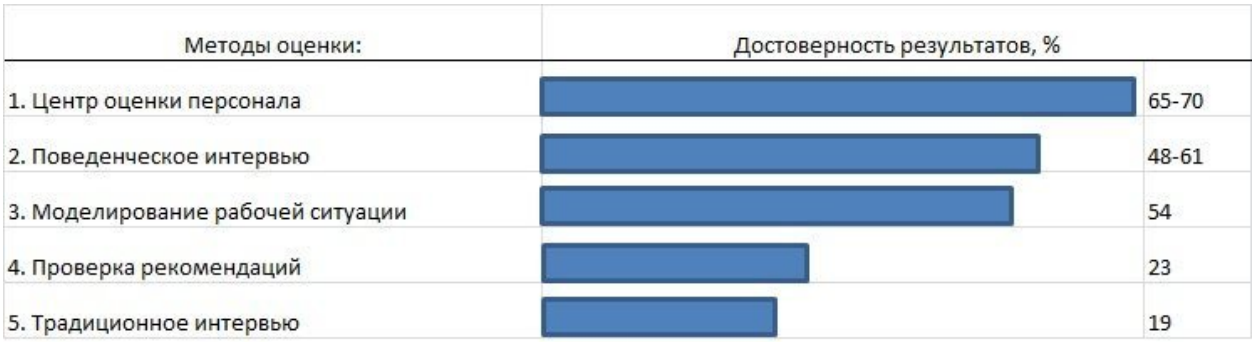

Рис. 1. Статистика достоверности результатов ассесмент-центра в процентах [7]

С помощью предлагаемого метода можно будет оценить не только готовность АГ в целом, но и готовность каждого участника АГ к проведению АИБ.

Рекомендации по адаптации существующих методов для решения поставленной задачи. Рассмотренные методы вполне можно адаптировать для применения в сфере АИБ. Данные методы положены в основу разработки алгоритма решения поставленной задачи по разработке методики оценивания готовности АГ к проведению АИБ. При этом саму задачу можно декомпозировать на ряд частных:

- анализ потенциала АГ;
- поддержание мотивации АГ;
- продвижение АГ;
- выявление некомпетентных участников АГ;
- разработка необходимых программ обучения;
- расчет затрат на развитие АГ;
- установление обратной связи с АГ;
- получение полной информации о готовности АГ к проведению АИБ.

Само оценивание готовности АГ к проведению АИБ может выглядеть в виде процесса, представленного на рисунке 2.

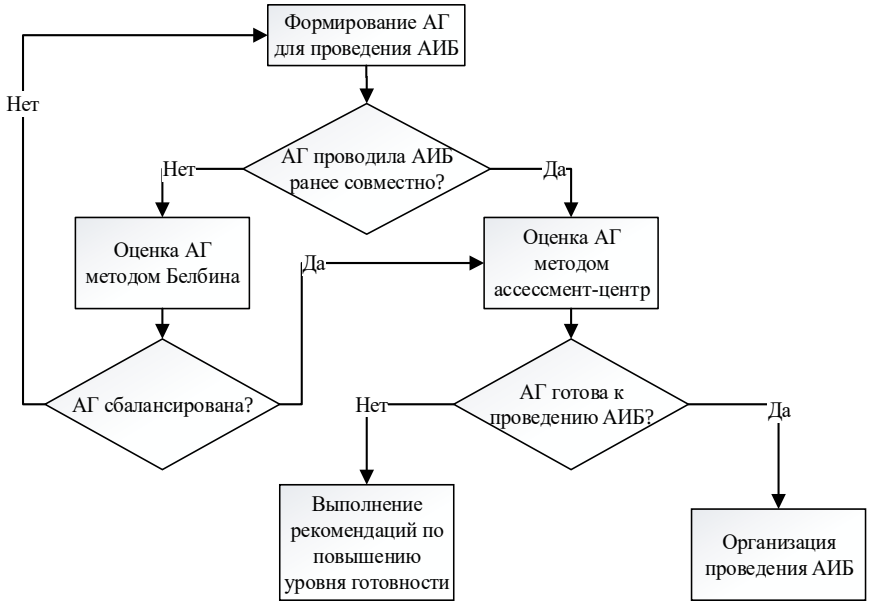

Рис. 2. Алгоритм оценки готовности АГ к проведению АИБ

Оценка АГ начинается с формирования самой АГ для проведения АИБ. В случае если АГ сформирована впервые в таком составе, то АГ должна пройти оценку методом Белбина на определение командных ролей у участников АГ. В случае если АГ ранее работала в таком составе, то АГ проходит оценку методом ассесмент-центр.

Оценка АГ методом Белбина включает следующие этапы:

1) назначение ответственного за проведение оценки АГ методом Белбина;

2) ознакомление членов АГ с методом Белбина;

3) заполнение каждым из участников АГ опросника по методу Белбина, самостоятельная обработка результатов.

4) предоставление результатов АГ ответственному за проведение оценки;

5) анализ командных ролей АГ ответственным за проведение оценки, определение сильных и слабых сторон АГ, потенциальных трудностей и возможностей;

6) принятие решения ответственным за проведение оценки о возможности эффективного взаимодействия АГ при проведении АИБ (о сбалансированности АГ);

7) предоставление результатов АГ.

В случае если АГ достаточно сбалансирована, то АГ группа проходит оценку методом-ассессмент центр, иначе АГ переформировывается.

Оценка методом ассессмент-центр включает следующие этапы:

1) Подготовительный: назначение ответственного за проведение оценки; назначение наблюдателей на время проведения оценки; разработка план-графика проведения оценки; выбор или разработка моделирующих упражнений; ознакомление АГ с методом оценки и план-графиком проведения оценки.

2) Основной: обеспечение проведения всех мероприятий в соответствии с согласованным планом-графиком.

3) Заключительный: проведение дискуссий среди наблюдателей; обобщение данных наблюдателей, подведение итогов; составление заключительного отчета с результатами по каждому участнику и всей АГ; проведение сессии обратной связи с каждым участником и всей АГ; предоставление рекомендаций по итогам оценки.

В случае если АГ показала хороший результат, готова к проведению АИБ, то АГ допускается до проведения АИБ, иначе АГ направляется на повышение уровня готовности, следуя рекомендациям, полученным по результатам оценки.

Заключение. Таким образом, в результате исследований была получена постановка задачи по разработке методического обеспечения оценивания готовности АГ к проведению практического аудита. Постановка задачи может быть востребована при разработке программы оценивания готовности АГ.

Библиографический список

1. ГОСТ Р ИСО 19011-2021 Руководящие указания по аудиту систем менеджмента. Пер. А. Горбунов, Номер для ссылки ISO 19011:2018.

2. ГОСТ Р ИСО/МЭК 27006-2008 Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности.

3. ГОСТ Р ИСО/МЭК 17021-1-2017. Оценка соответствия. Требования к органам, проверяющим аудит и сертификацию систем менеджмента. Часть 1. Требования.

4. Ефремова Н.Ф. Подходы к оцениванию компетенций в высшем образовании: Учеб. пособие. – М. Исследовательский центр проблем качества подготовки специалистов, 2010. – 216 с.

5. Максин Д.Г. 555 вопросов по компетентности руководителей проектов. Подготовка к сертификации в соответствии с требованиями IPMA/СОВНЕТ. – М.: ОЧУ ДПО «УКЦ «Проектная ПРАКТИКА», 2014. – 219 с.

6. Гуцыкова С.В. Метод экспертных оценок. Теория и практика. – «Когито-Центр», 2011. – 89 с.

7. Ассессмент центр как метод оценки персонала. – [Электронный ресурс]. – Режим доступа: https://hrhelpline.ru/assessment-tsentr-kak-metod-otsenki-personala/ (дата обращения 26.03.21).

ON SETTING THE TASK OF ASSESSING THE READINESS OF THE AUDIT GROUP TO CONDUCT AN INFORMATION SECURITY AUDIT

Yu.A. Nenasheva, *Graduate Student*
V.A. Voevodin, *Candidate of Technical Sciences, Associate Professor*
S.A. Kalishchuk, *Candidate of Medical Sciences, Associate Professor*
National Research University of Electronic Technology
(Russia, Moscow)

Abstract. *The results of the study of requirements to the competence of auditors and the readiness of the audit team, existing methods of assessing the competence of auditors and the readiness of the audit team are given. Research has been carried out on significant information infrastructure that operates under threat conditions. The results of the study showed that the possibilities of methodical support to assess the readiness of the audit team as a whole to conduct information security audits are insufficient for an objective assessment of the competence of auditors and the readiness of the audit team as a whole. It justifies a necessity in development of methods of assessment of competence of auditors and readiness of auditing group for information security audit. The article provides a statement of the research task, results of analysis of existing methods, algorithm of assessment of readiness of the audit group.*

Keywords: *audit, information security audit, audit group, readiness of audit group, audit program.*