DOI: 10.25728/avtprom.2020.03.05

Оценка риска поставщиков консалтинговых услуг в области информационной безопасности

И.И. Лившиц (Университет ИТМО)

Показано, что консалтинговые услуги являются востребованными среди отечественных промышленных предприятий, в том числе в области информационной безопасности. В случае привлечения консалтинговых компаний на первый план выходят проблемы контроля качества оказываемых услуг. Показано, что в области информационной безопасности создана мощная нормативно-правовая база, позволяющая обезопасить потребителей консалтинговых услуг от недобросовестных поставщиков. Сформулированы основные риски, с которыми могут столкнуться потребители консалтинговых услуг. Предложен простой математический аппарат для оценки и мониторинга этих рисков.

Ключевые слова: консалтинг, управление рисками, информационная безопасность, функциональная безопасность, аудит.

Введение

Консалтинговые услуги находятся сегодня на пике популярности. На определенном этапе развития организация сталкивается с проблемами, которые не может эффективно решить своими силами. На помощь приходят консалтинговые компании, которые оказывают профессиональную помощь, заключающуюся в совместно с заказчиком вырабатываемых решениях на основе анализа существующих проблем функционирования и определении путей дальнейшего развития конкретной организации.

Привлечение внешних консультантов имеет для организации ряд преимуществ. Так, в компании может не быть специалистов по отдельному направлению; внешним сотрудникам проще увидеть со стороны недостатки, к которым привыкли штатные специалисты; специалисты консалтинговых компаний имеют опыт работы и решения, проверенные при сотрудничестве с другими организациями.

В практике промышленно развитых стран вложение средств в приобретение интеллектуального капитала в форме услуг консультантов рассматривается как более эффективное, чем даже вложение средств в развитие технологий и приобретение оборудования [1–3].

При такой важности и затратности консалтинговых услуг для предприятий встает вопрос об оценке качества полученных консультаций, о практической пользе разработанных консультантами решений. Особенно это актуально применительно к отечественным предприятиям. Специалисты в области экономики отмечают неадаптированность существующих методик проведения консалтинговых работ к условиям экономики России, недостаток научно-методической литературы и нормативно-правовой базы [4].

В статье речь пойдет об оказании услуг в области информационной безопасности (ИБ). Отметим, что в России на данный момент существует достаточное число компаний, готовых оказать соответствующие консультационные услуги.

Нормативно-правовая база

Применительно к области ИБ проблем с отсутствием нормативно-правовых документов не наблюдается. Напротив, предлагается принять во внимание классические источники: например, ISO (ГОСТ Р ИСО) серии 27001 — для оценки требований информационной безопасности (ИБ) ISO (ГОСТ Р ИСО) серии 9001 — для оценки требований менеджмента качества, ISO (ГОСТ Р ИСО) серии 14001 — для оценки требований экологии, ISO (ГОСТ Р ИСО) серии 45001 — для оценки требований промышленной безопасности и ISO (ГОСТ Р ИСО) серии 50001 — для оценки требований энергоменеджмента. Кроме того, отметим стандарты в области управления аусорсингом ISO 37500 и менеджмента активов ISO 55001.

В настоящее время в РФ принятые новые нормативные акты, выполнение которых является обязательным, тогда как применение стандартов ISO и/или ISO/IEC может быть, в известной мере, добровольным. Это Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры РФ» и Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры РФ».

Все эти документы могут быть успешно применены при заключении договоров на консалтинговые услуги в области ИБ и оказать существенную помощь компаниям, которые эти услуги готовы заказать [5–7].

Кроме того, настоятельно рекомендуется включать в состав основных общих требований для целей обеспечения безопасности требования к функциональной безопасности на базе стандартов IEC серии 61508 (табл. 1).

Таблица 1. Требования к функциональной безопасности IEC 61508

Стандарт	Раздел	Пункт	Требование
IEC 61508-1	Управление функциональной безопасностью	6.1.2	Технические требования, необходимые для поддержания функциональной безопасности, определяются как часть информации, предоставляемой поставщиком Э/Э/ПЭ систем, связанных с безопасностью, их элементов и компонентов.
IEC 61508-2	Требования к реализации системы	7.4.9	Поставщик подсистемы или элемента, от которого требуется соответствие МЭК 61508, должен предоставить эту информацию разработчику системы, связанной с безопасностью (либо другой подсистемы или элемента) в виде соответствующего руководства по безопасности.
IEC 61508-2	Подтверждение соответствия безопасности системы	7.7.2.6	Поставщик или производитель должны сделать доступными результаты испытаний подтверждения соответствия безопасности электрических, электронных, программируемых электронных (Э/Э/ПЭ) систем производителю управляемого оборудования и систем управления управляемого оборудования с тем, чтобы позволить им обеспечить выполнение требований подтверждения соответствия всей системы безопасности в соответствии с МЭК 61508-1.
IEC 61508-3	Требования к проектированию архитектуры программного обеспечения	7.4.3	В соответствии с требованиями настоящего стандарта к поставщику может быть предъявлено требование гарантировать пользователю соответствие поставляемого продукта требованиям 7.4.
		7.4.3.2	Проект архитектуры программного обеспечения должен быть создан поставщиком программного обеспечения и/или разработчиком, описание архитектуры должно быть подробным. b) основываться на разделении на элементы/подсистемы, для каждой из которых должна предоставляться следующая информация: 1) проводилась ли верификация и если проводилась, то при каких условиях, 2) связан ли каждый из этих компонентов/подсистем с безопасностью

Дополнительно отметим термин «проверено в эксплуатации» (п. 3.8.18 IEC 61508-4), согласно которому требуется: «демонстрация, основанная на анализе опыта работы определенной конфигурации компонента, того, что вероятность опасных систематических отказов компонента настолько низка, что каждая функция безопасности, которую реализует этот компонент, достигает требуемого для нее уровня полноты безопасности».

Обратимся к опыту зарубежных регуляторов. Например, European Union Agency for Cybersecurity (ENISA) в феврале 2020 г. опубликовало руководство «Good practices for the security of Healthcare services» (Руководство по безопасности для медицинских сервисов) (www.enisa.europa.eu). Европейский регулятор рекомендует для оценки соответствия различного медицинского оборудования и сервисов требованиям безопасности множество самых разных нормативных документов: международные стандарты ISO, IEC, американские стандарты NIST и стандарт оценки Health Level — HL7 (табл. 2). Конечно, некоторые вопросы «применимости» международных стандартов для целей оценки ряда сервисов (в частности, облачных) могут быть предметом дискуссии, но в целом представленная таблица дает объективную картину важности оценки соответствия для безопасности медицинских объектов по множеству применимых стандартов.

Таблица.2 Требование соответствия медицинских сервисов стандартам по безопасности

Стандарты	Клинические информационные системы	Медицинские приборы	Сетевое оборудование	Системы удаленной диагностики	Мобильное клиентское устройство	Системы идентификации	Системы управления зданием	Промышленные системы управления	Профессиональные сервисы	Облачные сервисы
ISO 80001			X	X	X	X	X		X	
ISO 13972			X	X	X	X	X		X	
ISO 13485		X	X	X	X	X	X		X	
ISO 14971		X	X	X	X	X	X		X	
ISO / IEC 20000	X		X	X	X	X	X		X	
ISO 27000	X		X	X	X	X	X		X	
ISO 27799	X		X	X	X	X	X		X	
ISO 22857	X		X	X	X	X	X		X	
ISO 27019			X	X	X	X	X	X	X	
ISO 27017										X
IEC 62304	X		X	X	X	X	X		X	
IEC 60364-7-710			X	X	X	X	X	X	X	
ISA/IEC 62443			X	X	X	X	X	X	X	
DICOM			X	X	X	X	X		X	
HL7			X	X	X	X	X		X	
NIST-SP 800-66	X		X	X	X	X	X		X	
NIST CSF	X		X	X	X	X	X		X	
HTMs			X	X	X	X	X	X	X	

Риски поставщиков консалтинговых услуг

Как любой поставщик, консалтинговые компании (в том числе и представители мировой элиты — Deloitte, KPMG, Ernst & Young, PricewaterhouseCoopers и пр.) готовы оказать широкий спектр услуг, в том числе и в области обеспечения безопасности, но, как и любой поставщик, привносят и свои специфические риски. Будет правильным проводить объективный анализ осуществимости консалтингового проекта для конкретного объекта еще на стадии формировании тендерной

документации. И уже на этой стадии необходимо вводить четкие параметры контроля выполнения проекта для оценки всеми заинтересованными службами рисков, во-первых, и оценивать значения критериев экономической эффективности в виде соотношения результативности (в части достижения целевых функций ИБ — надежной, стабильной и бесперебойной работы) и затраченных ресурсов, во-вторых.

Определим значимые риски, с которыми могут столкнуться потребители консалтинговых услуг, и предложим простые параметры для их измерения и мониторинга.

1. Риск не обеспечения полноты требований функциональной безопасности решений, предлагаемых поставщиками консалтинговых услуг. Известно, что существуют «уникальные» продукты ведущих консалтинговых компаний. Каждый из них «заточен» под уже существующее решение, известное конкретным консультантам, привлекаемым на конкретный проект. Соответственно, возникает угроза недостаточного изучения проблемной области нового конкретного проекта и, соответственно, риск неполного (ошибочного) покрытия функций безопасности.

Предлагается оценить параметр:

$$K_1 = \frac{\sum C}{\sum T} * 100\ \%,$$

где: C — объем доработки функций безопасности существующего решения, T — общий объем реализованных функций безопасности в существующем решении.

При установленных ограничениях:

$$0 \leqslant K_1 \leqslant 1$$

следует, что при K_1, близком к 1, поставщик полностью адаптирует существующее решение под реальный объект, в том числе проводит экспертизу, формирует новый комплект документации, выполняет оценку соответствия и пр. При K_1, близком к 0, внедряется уже существующее решение, невзирая на функциональные, процессные, законодательные, организационные и иные особенности объекта у нового заказчика.

Отметим, что произведение K_1 и стоимости проекта (S) позволяет получить численную оценку риска и представить ее для согласования высшему менеджменту.

2. Риск возможности внедрения существующего решения при конкретных требованиях. Следует оценить заблаговременно, что персонал поставщика консалтинговых услуг обладает необходимыми знаниями в предметной области, в которой планируется оказать консалтинговые услуги. В наиболее негативном сценарии поставщик предложит минимальную цену, чтобы его стажеры учились именно на новом консалтинговом проекте.

Введем параметр:

$$K_2 = \sum_{i=1}^{n} \frac{R_i}{T_i} * N_i * 100\%,$$

где R_i — время адаптации (доработки) функций безопасности существующего решения, T_i — общее время фазы проекта в существующем решении, N_i — число консультантов, занятых в реализации фазы жизненного цикла в существующем решении, i — число фаз жизненного цикла для нового конкретного объекта.

При установленных ограничениях:

$$0 \leqslant K_2 \leqslant 1$$

следует, что при K_2, близком к 1, заказчик полностью оплачивает обучение команды консультантов под новый проект, а при K_2, близком к 0, поставщик внедряет готовое решение по схеме «как есть», невзирая на существующие функциональные, процессные, законодательные, организационные и иные особенности объекта у нового заказчика.

Следует признать, что практика «обкатки» как нового проекта, так и команды консультантов не является уникальным подходом, так как все консалтинговых компании стремятся как минимизировать издержки, так и максимизировать число стажеров на проекте, выбранном «полигоном».

3. Риск игнорирования современных требований безопасности со стороны консультантов как мера «консервации» существующего собственного решения и игнорирования применения методик, основанных на международных стандартах (ISO и/или ISO/IEC).

Введем параметр:

$$K_3 = \frac{\sum A}{\sum B} * 100\%,$$

где A — число новых требований безопасности, внесенных в существующее решение, B — общее число требований безопасности, определенных в международных стандартах.

При установленных ограничениях:

$$0 \leqslant K_3 \leqslant 1$$

следует, что при K_3 близком к 1, заказчик полностью оплачивает поставщику адаптацию (локализацию) существующего решения под конкретные требования безопасности, определенные в международных, отраслевых и национальных стандартах. При K_3, близком к 0, поставщик внедряет готовый, примерно подходящее решение, представляющее собственные методики, не сопоставимые с актуальными и признанными мировым экспертным сообществом требованиями безопасности.

Пример выявленных рисков поставщиков консалтинговых услуг

Обратим внимание на важность каждой мелочи, способной негативно повлиять на успешное создание системы безопасности промышленного объекта. Например, это может быть и небрежно оформленные сертификаты компетентности экспертов (а более критические приложения могут потребовать про-

Об услуге пусть рассказывает не оказавший, а получивший её.
Луций Анней Сенека (младший)

верки номера сертификата и лицензий организации, выдавшего конкретный сертификат), так и общую компетентность поставщика, претендующего на оказание конкретных консалтинговых услуг.

Например, в одном из проектов по созданию и оценке безопасности объекта в пакете тендерной документации был представлен сертификат «ведущего аудитора» на соответствие ISO 9000, то есть словаря, а не ISO серии 9001, как полагается. Другим примером могут служить грамматические ошибки в презентациях и представляемых клиенту документах.

В связи с этим настоятельно рекомендуется еще до начала выполнения проекта оценить степень зрелости привлекаемых поставщиков (как рекомендуют стандарты ISO) и принять взвешенное решение о целесообразности их привлечения к консультированию собственной компании.

Отдадим дань уважения фундаментальным научным трудам, в которых при пристальном изучении можно найти подтверждение предложенному подходу оценки рисков оплаты новых предлагаемых сущностей. В частности, в работе Н. Винера отмечается: *«Разумеется, подобно тому, как квалифицированный плотник, квалифицированный механик или квалифицированный портной пережили так или иначе первую промышленную революцию, квалифицированный ученый и квалифицированный администратор могут пережить и вторую. Но представим себе, что вторая революция завершена. Тогда средний человек со средними или еще меньшими способностями не сможет предложить для продажи ничего, за что стоило бы платить деньги»* ([8], стр. 79). Это утверждение как нельзя точно определяет подход к оценке рисков всех рассмотренных выше примеров и позволяет принять решение о приемлемости всего, что «предлагается для продажи» в конкретном проекте.

Выводы

Проблема оценки рисков поставщиков, оказывающих консалтинговые услуги, является весьма важной и требует применения методов управления специфическими рисками в процессах обеспечения информационной безопасности. Приведены примеры введения численных параметров, позволяющих получать объективные оценки деятельности поставщиков консалтинговых услуг на каждой стадии жизненного цикла объекта в соответствии с рекомендациями стандартов, например, ISO и/или IEC. Эти оценки могут послужить достаточной доказательной базой для высшего менеджмента в процессах обеспечения информационной безопасности. Полученные результаты могут быть применены на практике для оценки и мониторинга стоимости текущих и перспективных консалтинговых проектов.

Список литературы

1. *Забайкин Ю.В., Заернюк В.М.* Совершенствование механизма устойчивого развития промышленного предприятия: теория и методология. М.: Научные технологии, 2017. 263 с.
2. *Рябов А.А.* Проекты руководств по безопасности на опасных производственных объектах нефтегазового комплекса // Безопасность труда в промышленности. 2014. 12. стр. 68-70.
3. *Ермолина Л.В., Ильина Л.А.* Особенности управления проектами акселерации развития бизнеса нефтегазовых предприятий // Известия Волгоградского государственного технического университета. - 16 (195). 2016. стр. 80-84.
4. *Исрафилов Н.Т., Гарявин А.Н., Кецян С.М.* Российский современный консалтинг: решение проблем // Электронный научно-методический журнал Омского ГАУ. 2016. №2.
5. *Лившиц И.И.* Методика выполнения комплексных аудитов промышленных объектов для обеспечения эффективного внедрения систем энергоменеджмента // Энергобезопасность и энергосбережение. 2015. Вып. 3. С. 10-15.
6. *Livshitz I.I., Lontsikh P.A., Kunakov E.P.* Application of a hybrid method for key energy facilities safety assessment // EAI Endorsed Transactions on Energy Web. 2019. Vol. 19. Num 22.
7. *Livshitz I.I., Neklyudov A.V., Lontsikh P.A.* Evaluation of IT-security – genesis and its State-Of-Arts // Journal of Physics: Conference Series. Сер. "International Conference Information Technologies in Business and Industry 2018 - Enterprise Information Systems" 2018. P. 042029.
8. *Винер Н.* Кибернетика, или управление и связь в животном и машине. 2-е издание. М.: Наука; Главная редакция изданий для зарубежных стран. 1983. 344 с.

Лившиц Илья Иосифович *– д-р техн. наук, Университет ИТМО (Санкт-Петербург).*
E-mail: Livshitz.il@yandex.ru