ПРАКТИКА УПРАВЛЕНИЯ КИБЕРРИСКАМИ В НЕФТЕГАЗОВЫХ ПРОЕКТАХ КОМПАНИЙ ХОЛДИНГОВОГО ТИПА

Лившиц И.И.[1]

Цель работы: *анализ существующих подходов к управлению киберрисками и разработка рекомендаций для обеспечения информационной безопасности в нефтегазовых проектах компаний холдингового типа.*

Метод исследования: *применяются методы системного анализа и методы теоретико-сравнительного анализа. Исследуются риски, возникающие на различных стадиях подготовки нефтегазовых проектов.*

Результат: *разработана система выявления источников, идентификации и анализа киберрисков, способных повлиять на реализацию нефтегазовых проектов для компаний холдингового типа. Рассмотрены стадии жизненного цикла и отмечена необходимость обеспечения информационной безопасности при привлечении консалтинговых компаний.*

Рекомендуется обращать внимание на степень зрелости привлекаемых консалтинговых компаний. Обеспечение информационной безопасности предложено реализовывать на разных уровнях: при оценке компетенций специалистов, применяемых ИТ, культуры анализа и подготовки отчетных документов. Результаты проведенного исследования получили практическое применение при реализации нефтегазовых проектов.

Ключевые слова

Нефтегазовый проект, риски, система управления, интегрированная система управления, информационная безопасность, аудит.

DOI:10.21681/2311-3456-2020-01-42-51

Введение

Значительная часть проектов по разработке систем управления киберрисками (СУКР) в нефтегазовых проектах (НГП), либо полностью не приводит к ожидаемым результатам, либо в действительности требует затрат больших ресурсов, чем планировалось. Одна из причин данной ситуации, как представляется, заключается в отсутствии в распоряжении высшего менеджмента и команды проекта надежных методов управления рисками. В большей степени это утверждение справедливо в отношении корректного выбора и правильного применения в практике НГП апробированных инструментов управления киберрисками.

В представленной публикации рассмотрен пример значительного по длительности НГП, для которого выполнялась разработка СУКР. Определенное внимание уделено привлечению консалтинговых компания в НГП, рассмотрены несколько примеров. Показаны примеры выбора и применения различных инструментов управления киберрисков на всех стадиях жизненного цикла НГП в компаниях холдингового типа.

Обзор существующего терминологического аппарата

Для цели данной публикации необходимо исследовать существующий терминологический аппарат для формирования ясных сущностей и анализа их взаимосвязей в проекте СУКР применительно к области НГП. Предлагается следующее определение нефтегазового проекта (НГП) – *деятельность компании в рамках соглашения о разделе продукции, концессионного соглашения, соглашения о принципах проведения геологического изучения недр, меморандума, протокола, соглашения о совместной деятельности и иных соглашений в области разведки и добычи углеводородного сырья*.

Очевидно, что должны быть приняты во внимание не только классические источники (например, ISO[2]), но и ряд экспертных площадок, способных помочь в формировании согласованной терминологии [1 – 10]. Примеры расхождения терминологии в нормативных документах РФ (в частности, для терминов «*контролируемая зона*», «*инцидент*», «*доступность информации*»

1 Лившиц Илья Иосифович, доктор технических наук, доцент факультета безопасности информационных технологий Университет ИТМО, г. Санкт-Петербург, Россия. E-mail:Livshitz.il@yandex.ru

2 https://www.iso.org/ru/standard/54534.html

известны: в документах ФСТЭК «Базовая модель угроз», ГОСТ Р ИСО/ТО 13569-2007, ГОСТ Р 53114-2008, стандарт ГОСТ Р 57580.1-2017 и пр.). Предлагается в качестве «отправного пункта» взять описания бизнес-процессов, которые нацелены на получение добавленной стоимости (не только по отношению к внешнему потребителю, в частности[3]) [5 – 8]. Есть основания полагать, что бизнес-процесс, как ценный актив современной проектной организации, подвержен рискам и, в частности, киберрискам [10 – 14]. Рассмотрим текущее состояние исследования киберрисков для управления НГП с приложением области информационной безопасности (ИБ).

1. Русско-американский словарь терминов и определений[4] в сфере обеспечения кибер-безопасности, подготовленный совместными усилиями экспертов Института информационной безопасности при МГУ (РФ) и EastWest Institute (США), содержит определение кибербезопасности, как свойства киберпространства (киберсистемы) противостоять намеренным и/или ненамеренным угрозам, а также реагировать на них и восстанавливаться после воздействия этих угроз. Но определения киберрисков нет.
2. В руководстве «Кибербезопасность. Типовой учебный план»[5] представлено определение, разработанное для Министерства внутренней безопасности (США): «Кибербезопасность – это деятельность или процесс, способность, возможность или состояние, при которых системы информации и связи и информация, содержащаяся в них, защищены и/или охраняются от вреда, несанкционированного использования, модификации или эксплуатации». В тексте упоминаются кибериски (см. стр. 18 и 55) в общем описательном контексте, а точного определения не представлено. В словаре данного руководства термина «киберриск» нет.
3. В обзоре компании Gartner[6] предложен оригинальный подход, согласно которому экспертам по безопасности следует использовать термин «Cybersecurity» (кибербезопасность) исключительно для обозначения практических методов безопасности, сочетающих в себе меры наступательного и оборонительного характера, как совокупность системы информационных и/или операционных технологий. Но определения киберрисков нет.
4. Термин «Cybersecurity» (кибербезопасность) приводится в документе ITU-T Recommendation X.1205 «Overview of cybersecurity»[7], как набор инструментов: политик, концепций, мер защиты, подходов риск-менеджмента, обучения, лучших практик, технологий для защиты активов пользователя и организаций. Примечательно, что в представленной широкой трактовке данного термина упомянуты подходы риск-менеджмента (в оригинале: «*risk management approaches*»), но более детального толкования непосредственно для определения киберриска не представлено.
5. Документ «Cybersecurity Supervising a Moving Target»[8], содержит рекомендации в области кибербезопасности применительно к финансовой (банковской) сфере. Несмотря на наличие значительного объема аналитических данных (по состоянию на 2016 г.) и рекомендаций по общим принципам управления ИТ-рисками и ИБ-рисками, детальных подходов к управлению именно киберрисками не представлено. Даны только общие замечания о том, что киберриски характеризуются отсутствием всяких стандартов и руководств (*Guidance/Standard*) и отражена точка зрения, что киберриски могут управляться, но никогда не могут быть исключены. Данный документ не содержит необходимых определений.

С учетом рассмотренных выше результатов исследования трактовок киберрисков, введем новое определение киберриска – *это риск, связанный с использованием технологий, оборудования и программного обеспечения (ПО), в том числе при управлении НГП.* Для оценки киберрисков применяют различные «практические» стандарты (например, ISO 31010, ISO 27005, NIST SP-800-53 и пр.).

Проблемные области

Представляется целесообразным сформировать видение тех проблемных областей, влияние которых весьма существенно на НГП, для изучения которых следует создавать СУКР [15 – 22]. На практике владельцы бизнес-процессов требуют от специализированных подразделений компании (ИТ-службы, ИБ-службы, службы внутреннего аудита (СВА) и пр.) описания проблемных областей (иначе говорят «бутылочных горлышек»), в которых указанные процессы не достигают цели, и, соответственно, возможны потери. Под термином «потери» понимаются нет только финансовые издержки. Соответственно, для проблемных областей понимаем следующее: в НГП определен порядок, нарушение которого (и в равной мере появление угроз нарушения) должно предупреждаться специальными процедурами (в рамках систем менеджмента) еще «на подходе». В качестве таких систем менеджмента рассматриваются системы менеджмента информационной безопасности (ISO 27001), системы менеджмента непрерывности бизнеса (ISO 22301), системы менеджмента ИТ-услуг (ISO 20000:1) и интегрированных систем менеджмента (ИСМ). Представляется целесообразным определение следующих проблемных областей, исходя из имеющего опыта реализации сложных НГП:

1. *Срыв сроков производственных задач* – появление новых технологий предоставляет новые возможности, но и новые риски, которые с большой вероятностью включают кибериски, поскольку затрагивают любые компоненты ПО.

3 https://www.iso.org/ru/standard/73906.html

4 https://digital.report/cybersecurity-terminology/

5 https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/20171004_1610-cybersecurity-curriculum-rus.pdf

6 http://bis-expert.ru/blog/5345/42757

7 www.itu.int/dms_pub/itut/oth/0A/0D/T0A0D00000A0002MSWE.doc

8 http://pubdocs.worldbank.org en/968221477065129639/17-Cyber-Security.pdf

2. *Сложные ИТ* – в территориально-распределенных системах работают сотни коллег, что существенно расширяет проблемную область для проявления киберрисков, например, появления единой точки отказа и/или прекращения сервисной поддержки зарубежного ПО, факты которых широко известны.
3. *Сложное оборудование* – не всегда есть возможность контролировать выделенную стойку в удаленном ЦОДе, а многие компоненты ПО работают в «облаке».

Подходы

Известны несколько подходов создания СУКР, часть которых предлагается рассмотреть в качестве «хороших практик» для НГП:

- Подход ISO, в рамках которой внедряются как отдельные системы менеджмента (по данным ISO всего выполнено свыше 1 млн. внедрений СМК по ISO 9001, свыше 39 тыс. – ISO/IEC 27001 и свыше 5 тыс. – ИТ по ISO/IEC 20000:1). Но из всех проектов только 12% внедрили и оценивали ИСМ, в основном – предприятия пищевой промышленности;[9]
- Подход к унификации стандартов, определенный Всесоюзным комитетом по стандартизации СССР (в 1940 – 1946 гг. возглавлял В.С. Емельянов), согласно которому отклонялись проекты стандартов, показатели которых ориентировались на одну отрасль без учета остальных. Например, в 1943 г. было утверждено 488 стандартов, а 71 проект был отклонен.[10] Сейчас в РФ, к сожалению, отсутствует система научных исследований в области стандартизации;
- Подход NASA (модель «цифровых двойников», предложенная в 2002 г. М. Гривзом, которая затрагивает применение зеркалированной информации при управлении сложными объектами в течении всего ЖЦ), методы машинного обучения и статистического моделирования. Наибольшее значения имеют «операционные двойники», но это требуется Пфлопс на серверах высокой производительности;
- Решения класса GRC (*Governance, Risk, Compliance*), предложенные разработчиками (например, RSA, Oracle, SAP, RVision), пока не находят широкого применения в силу фрагментарного охвата функций ИБ, сложности внедрения, обязательным участием многочисленного персонала и высокой стоимости совокупного владения;
- Зарубежные методики (ISAGO, ITIL, COBIT, Octave, RiskIT, Harmonized TRA Methodology и пр.) уделяют внимание проблеме обеспечения ИБ, однако, единой концепции, увязанной с фазами ЖЦ и процессами обработки остаточных рисков ИБ к настоящему времени не представлено.

Можно привести цитату, весьма точно описывающую существующий порядок управления киберрисками: «*Предпринимаются попытки не просто вывести цифровизацию из-под научного аудита*»[11]. Соответственно, если существующих подходов недостаточно, многие уважаемые заказчики полагают возможным и целесообразным обратиться к известным консультантам с мировым именем.

Консультанты «Большой четверки»

Определенно, консультанты известных компаний (Deloitte & Touche, PricewaterhouseCoopers, Ernst & Young, KPMG, Accenture, Boston Consulting Group и пр.) готовы предложить свои фирменные методики управления, но это не дает гарантий, что для конкретной деятельности НГП это применимо. Проблема управления киберрисками еще больше усугубляется при объективном анализе осуществимости и критичных факторов успеха для НГП в компаниях холдингового типа. Однако, при выборе консультантов даже на стадии формировании тендерной документации не все факторы могут быть учтены исходя из уже имеющегося опыта. Как известно, «генералы всегда готовятся к прошедшей войне». Следует принять во внимание ранее определенные «проблемные области»: к чему точно должны быть готовы представители заказчика (ИБ, ИТ, СВА, ИСМ) при выборе консультанта по вопросу создания СУКР? Попробуем разобраться на конкретных примерах.

Риски, которыми не управляют консультанты по киберрискам

На основании опыта реального НГП представим значимые риски:

1. Выявление, идентификация и оценивание киберрисков – существуют «уникальные» фирменные методики ведущих консалтинговых компаний. Каждая из них «заточена» под уже существующий «кейс», известный конкретным консультантам. Никто не будет разбираться в ваших проблемах на конкретном НГП.
2. Какими киберрисками нужно управлять – состав команды консультантов состоит, традиционно, из 1 «боевого индийского слона» и мелкой «пехоты». Никто не гарантирует, что все знают, чем отличается QWASP от CVE, что такое Residual risk и как следует обрабатывать Intangible asset. Они будут учиться на вашем проекте.
3. Культура управления киберрисками – мышление любого консультанта основано на минимизации времени, затраченного на решение вашей проблемы и максимального использования уже готовых «кейсов».
4. Рассмотрим такие кейсы, выявленные в реальном НПГ:
   - На первом же интервью в 2018 г. представлен шаблон «Руководства по качеству» на базе ISO 9001 версии 2000 г., более того, настаивали, что он обязательный;
   - Никогда не слышали о международных стандартах аудита ISO серии 19011 и 17021;
   - Представили в пакете тендерной документации

9 Салимова Т.А. и др. Векторы развития СМК. Стандарты и Качество № 8(974) 2018 г. стр. 44 – 48

10 РГАЭ. – Ф. 4460. – Оп. 1. – Д. 118. – Л. 4 об

11 http://nvo.ng.ru/realty/2019-04-26/3_1043_ai.html

сертификат «эксперта» на соответствие ИСО 9000, т.е. словаря (см. рис. 1).

- Представлены «рекомендации» типовых шаблонов процедуры (входами являются и план аудита, и отчет по аудитам и план корректирующих действий), и описание одного из бизнес-процессов, в которых есть входы, но нет выходов (рис. 2).

Certificate of Achievement

This is to certify that

[redacted]

has successfully completed the course assessment and examination for the

ISO 9000:2000 Series Auditor/Lead Auditor Training Course

which is certified by the Governing Board of the Institute of Quality Assurance (IQA), International Register of Certificated Auditors (IRCA) and is compliant with the training requirements of the International Auditor and Training Certification Association (IATCA) for certification as an

IATCA QMS Auditor/Senior Auditor

and as an

IRCA QMS Auditor/Lead Auditor and Internal Auditor

Held on: *24th – 28th February 2003* at: *Moscow, Russia*

Signed: Training Manager Date: *27 May 2003*

Certificate Serial No: *LA2/03/RU/3510* Course Certification No: *A 17024*

Рис. 1. Пример «сертификата» эксперта на соответствие словарю ISO 9000

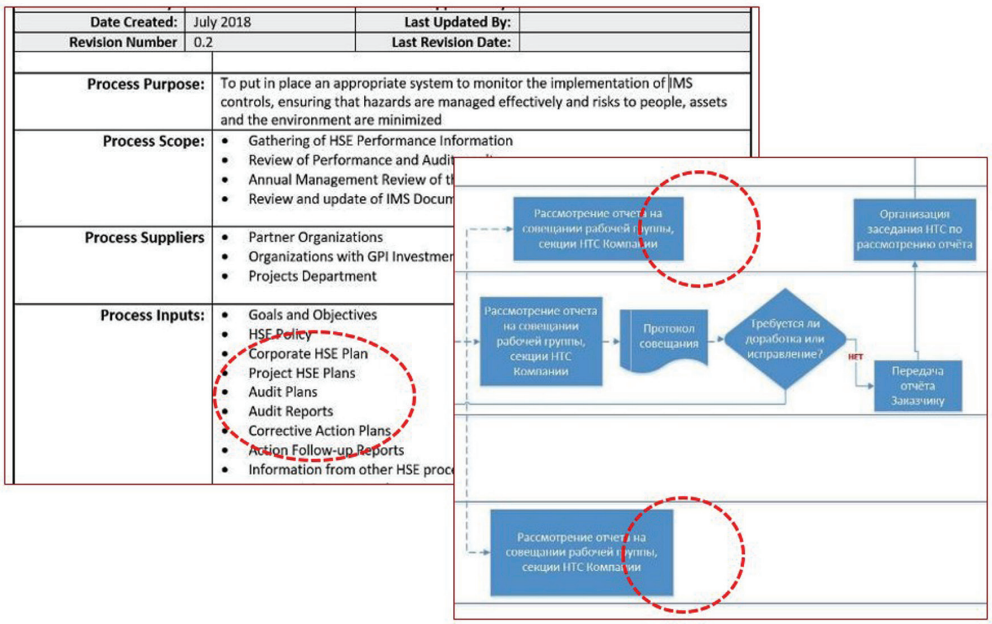
Очевидно, что такой подход ни в малейшей степени не позволяет достичь цели проекта по созданию СУКР, а только бы усилил существующую неопределенность (см. ISO 31000). Представляется возможным заметить еще один важный нюанс: явные попытки консультантов избежать применения отработанных методик, основанных на международных стандартах (ISO/IEC серии 38500[12] и 37500[13]).

- Рассмотрим пример нарушения политики «чистого стола и чистого экрана» (см. рис. 3) – безнадзорно оставленные документы (в том числе, содержащие чувствительную информацию), незаблокированный компьютер и смартфон, хотя консультанты работают в общем помещении, доступ в которое есть у различных работников компании (в том числе, у потенциальных посетителей).

Соответственно, до начала выполнения проекта создания современной СУКР для НГП необходимо оценить степень зрелости привлекаемых консультантов и принять решение о том, какой инструментарий следует применять.

Инструментарий риск-менеджера

С учетом негативного опыта общения с консультантами (в том числе, по указанным выше примерам), команда риск-менеджмента НГП приняла решение о создании СУКР в составе известных стандартов ISO серии 9001, 14001, 27001, 45001, и дополнительно: ISO серии 19011, 31000, 38500 и 37000. С учетом практики было определено, что требуется два набора инструментов при реализации НГП в компании холдингового типа:



Date Created:	July 2018	**Last Updated By:**	
Revision Number	0.2	**Last Revision Date:**	
Process Purpose:	To put in place an appropriate system to monitor the implementation of IMS controls, ensuring that hazards are managed effectively and risks to people, assets and the environment are minimized		
Process Scope:	• Gathering of HSE Performance Information • Review of Performance and Audit • Annual Management Review of t • Review and update of IMS Docun		
Process Suppliers	• Partner Organizations • Organizations with GPI Investmer • Projects Department		
Process Inputs:	• Goals and Objectives • HSE Policy • Corporate HSE Plan • Project HSE Plans • Audit Plans • Audit Reports • Corrective Action Plans • Action Follow-up Reports • Information from other HSE proc		

Рис. 2. Примеры «типовых» решений консультантов

12 ISO 38500:2015 – Information technology – Governance of IT for the organization

13 ISO 37500:2014 – Guidance on outsourcing

1. «Малый набор» - для быстрого старта проекта создания «контекста» СУКР:
   - ISO 31000 (31010) версии 2018 (2019),
   - ISO/IEC 27005 версии 2018,
   - NIST SP-800-53.
2. «Большой набор» - для обеспечения дальнейшего развития СУКР в рамках ИСМ:
   - ISO серии 19011 – для выполнения аудитов,
   - ISO серии 31000 (31010) – для управления рисками,
   - ISO серии 38500 – для управления ИТ,
   - ISO серии 37000 – для управления аутсорсингом.

Управление киберрисками в фазах цикла PDCA

Для целей данной публикации важно, что все предположения, заявленные командой НГП в начале ЖЦ, проверяются в полной мере в процессе планового внутреннего аудита ИСМ с установленной периодичностью. В полном объеме проверяется адекватность определения внутреннего и внешнего контекста, а также всего комплекса технических решений и мер обеспечения ИБ в соответствии с ранее установленными целями НГП. Для данных целей применяется СУКР, созданная для оперативного управления указанными ранее компонентами и, в равной мере, для системного изменения внутренней нормативной документации и перераспределения ресурсов. Пример СУКР, реализованных в фазе Check («проверяй») цикла Деминга показан на рис. 4.

Замысел разработки СУКР

С учетом негативного опыта работы консультантов, замысел разработки СУКР был определен в обеспечении системного подхода при выполнении НГП (см. рис. 5).

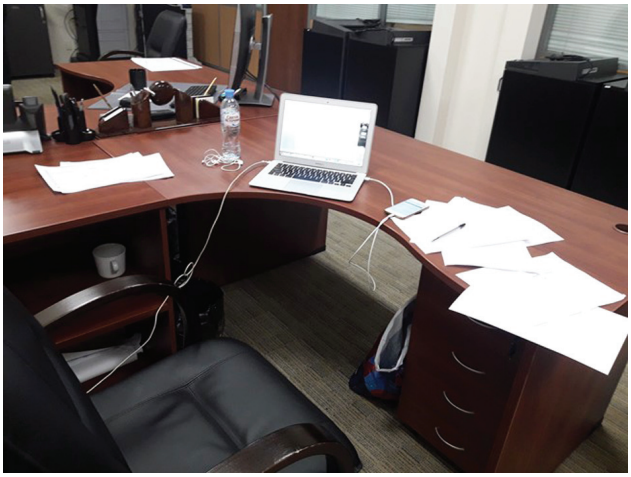


Рис. 3. Пример нарушения политики «чистого стола и чистого экрана» консультанта

Одним из преимуществ является учет различных интересов в компаниях холдингового типа, в частности, при реализации территориально распределенных, технически и технологически сложных НГП в ограничениях внешних негативных воздействий. В этих условиях владелец НГП требует обеспечить достижение заданной цели проектной команды, при этом обеспечивая качество реализации НГП. В обобщенное понятие «качество реализации» входит широчайший спектр требований, в том числе, аспекты ИБ. Следующим важным фактором является не раздельное достижение «локальных» целей (сначала, например, цель в области ИБ, потом цель в области СМК и пр.) и потом достижение «глобальной»

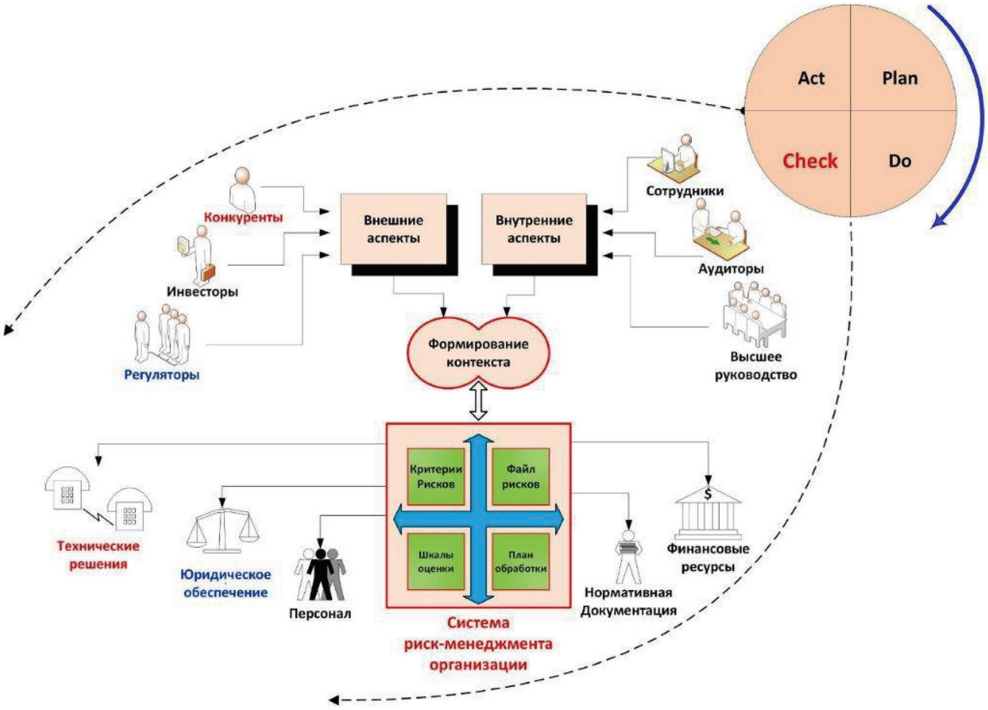


Рис. 4. Управление рисками в цикле PDCA (Фаза Check)

цели для всего НГП в компании холдингового типа, а построение ИСМ, в которой обеспечивается достижение единой цели, с учетом, соответственно, всех известных ранее ограничений, возмущающих воздействий, и, безусловно – совокупности рисков под управлением СУКР (см. рис. 5). Уместно предоставить дополнительные пояснения, прежде всего в части различий между понятиями «система управления» и «системы менеджмента», которые чаще всего вызывают сложности практического применения (см. Таб. 1).

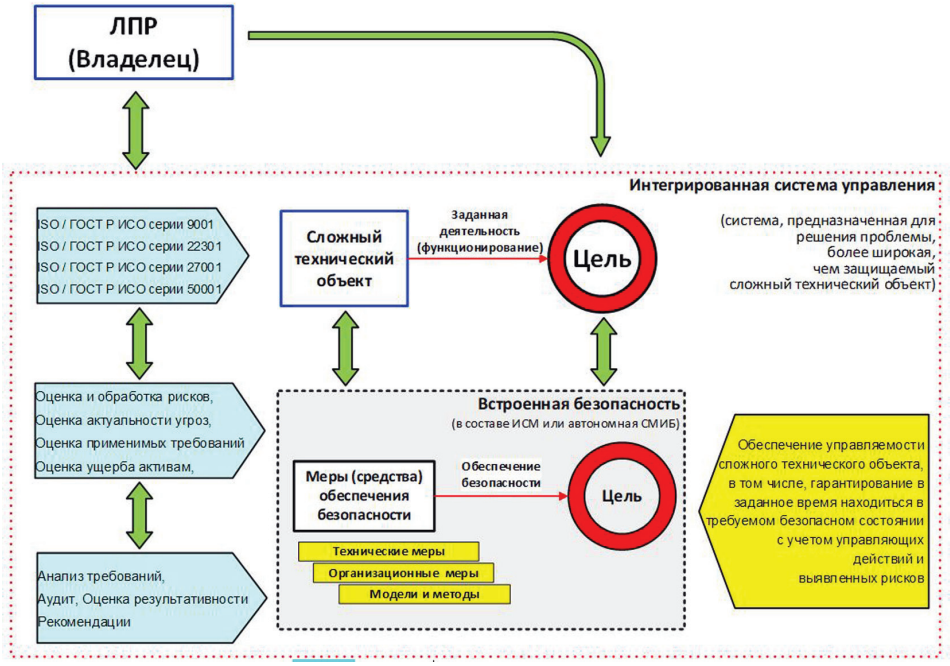


Рис. 5. Замысел разработки СУКР

Таблица 1.

Соответствие различий между системой управления и системами менеджмента

Сущность	Система управления	Системы менеджмента
Реализация объекта	СУ (Интегрированная СУ)	- Система менеджмента качества - Система менеджмента непрерывности - Система менеджмента ИБ - Система менеджмента ИТ-сервисов - ИСМ (интегрированная)
Ограничения	ЛПР (директор)	- Руководители функции (процесса) - Представители руководства (ПРК,..)
Достижение цели	Бизнес-цели	- Соответствие требованиям применимого законодательства - Выполнение критических факторов успеха (KPI)
Требования	Бизнес	- ФЗ (63, 98, 102, 149, 152, 184, 187,...) - ФСБ (ФСТЭК) - СТО БР ИББС (СТО Газпром СОИБ) - PCI DSS, GDPR и пр.
Подходы к управлению	Принятая бизнес-практика	- Оценка рисков - Лучшие имеющиеся технологии - Отраслевые рекомендации (требования)

DOI:10.21681/2311-3456-2020-01-42-51

Интегрированные системы менеджмента

На практике НГП обеспечивается «единое управляющее поле» (можно сравнить с методологией ИСМ) для обеспечения успешной и устойчивой проектной деятельности компании, а также учета лучшей практики в сложной конкурентной обстановке нефтегазовых компаний. Следует заметить, что в рассматриваемом НГП изначально в первых фазах ЖЦ уделялось большое внимание соответствию современным требованиям стандартов ISO, даже когда некоторые из них в 2017-2018 гг. были в статусе проектов (FDIS), и это требование было неукоснительно перенесено в тендерную документацию.

Одним из ключевых факторов успеха в рассматриваемом НГП по внедрению эффективной СУКР является обеспечение поддержки современными ИТ ([13, 14]). Соответственно, были дополнены требования в части обеспечения ИБ, особенно при разделении передачи информации между внутренним и внешним периметром (см. рис. 6). С учетом известных факторов успеха в рассматриваемых НГП было уделено особое внимание необходимости достижения эффекта эмерджентной системы – органичной интеграции всех рабочих органов компании в «единое управляющее поле» ([13, 14]). Соответственно, по аналогии, ИСМ формирует мягкие условия для создания эффективной корпоративной СУКР, влияющей на устойчивое выполнение НГП, или, по аналогии: «управлении в большом» и «управлении в малом» (как показано в ряде работ Месаровича, Мако и Такахара), подчеркивая создание правил и контроль выполнения этих правил.

Риски проекта создания СУКР

Создание современной СУКР, разработанной для обеспечения управления НГП, значительно отличается от тривиальных задач по созданию простейших СМК, которые хорошо известны в мире и в практике крупнейших российских компаний, например, ПАО «Газпром»[14]. Действительно, многие компании группы ПАО «Газпром» демонстрируют успехи в процессе освоения не только СТО Газпром серии 9001, но и соответствие требованиям международных стандартов. Особенности проблемы создания СУКР состоят в том, что в качестве объекта управления находятся не хорошо известные процессы добычи, транспортировки, переработки и сбыта углеводородного сырья и нефтепродуктов, а объекты инвестиционного нематериального поколения. Следует обеспечить учет значительного количества факторов, в стандартах ISO именуемых «внешним контекстом» и «внутренним контекстом» и обеспечить поддержку ИСМ с помощью СУКР. Как показывает анализ публикаций и докладов на специализированных форумах: Байкальский риск-форум[15] и Петербургский международный газовый форум[16], присутствует понимание, что система риск-менеджмента не может жить отдельно от ИСМ. В обеспечение данного тезиса можно привести достаточно предложений от компаний (IBM, EMC, RSA, SAP, Oracle и пр.), и заслуживает особое внимание предложение новых подходов, называемых «цифровыми двойниками» (можно отменить доклады на ПМГФ-2018 Siemens, AVEVA и пр.).

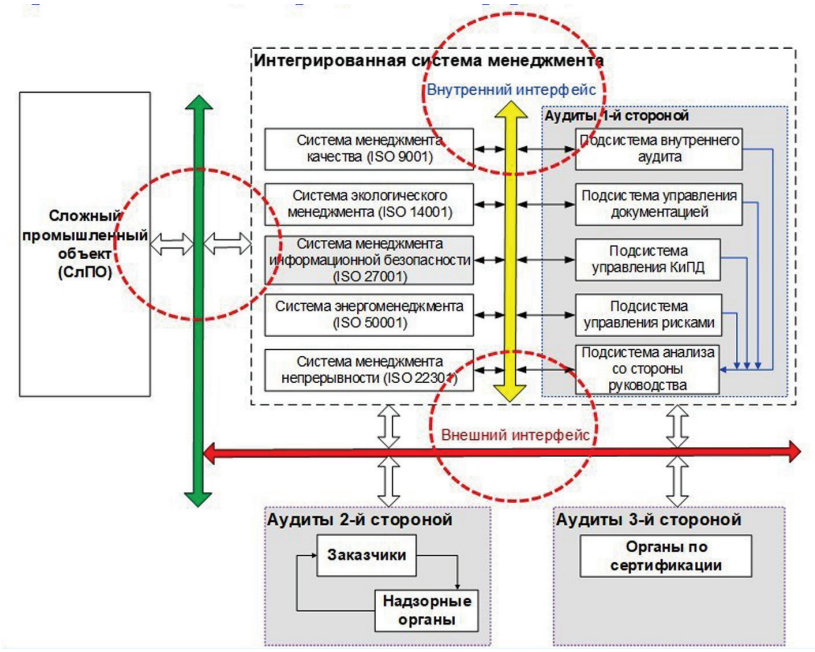


Рис. 6. Разделение информации в ИСМ компании

14 http://moskva-tr.gazprom.ru/about/manage/

15 https://www.ibrif.ru/

16 http://gas-forum.ru/

В рамках СУКР удалось реализовать еще одну грань интеграции: киберриски были интегрированы в «единое управляющее поле» компании при выполнении НГП. Внедрения стандартов ISO/IEC серии 27001 и/или 20000 уже объективно недостаточно и нужно переходить к новым стандартам, например, управления знаниями (*Knowledge management*), например, на базе ISO 30401[17]. В подтверждение данного тезиса можно привести пример анализа фрагмента технико-экономического обоснования НГП с учетом корпоративной системы менеджмента знаниями (см. на рис. 7).

Вывод

При создании СУКР для выполнения НГП в компаниях холдингового типа необходимо создавать ИСМ в составе известных стандартов ISO серии 9001, 14001, 27001, 45001 и пр., а также учитывать новые перспективные стандарты ISO, например, серии 37500, 38500 и 30401. Эти требования должны быть максимально учтены в случае приглашения консалтинговых компаний, для которых процедуры управления киберрисками должны устанавливаться и контролировать с самой ранней стадии ЖЦ. Представленная работа отражает общие итоги исследования, получившего практическое подтверждение при реализации НГП в 2017-2019 гг. и удостоена диплома лауреата 1-й премии на Международном конкурсе научных, научно-технических и инновационных разработок, направленных на развитие топливно-энергетической и добывающей отраслей[18] в 2019 г.

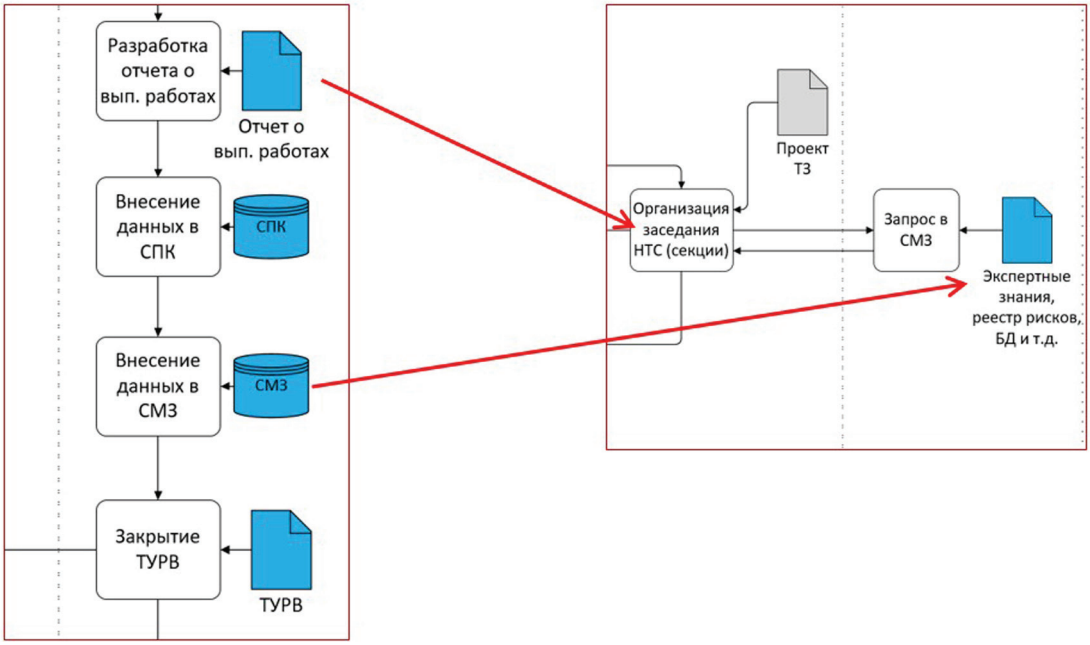


Рис. 7. Пример применения Системы менеджмента знаниями при управлении НГП

Рецензент: *Молдовян Александр Андреевич, начальник научно-исследовательского отдела проблем информационной безопасности, доктор технических наук, профессор, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), Санкт-Петербург, Россия. E-mail: maal305@yandex.ru*

17 ISO 30401:2018 Knowledge management systems. Requirements

18 https://www.technodevelop.ru/

Литература

1. Teilans A.A., Romanovs A.V., Merkuryev Yu.A., Dorogovs P.P., Kleins A.Ya., Potryasaev S.A. / Assessment of Cyber Physical System Risks with Domain Specific Modelling and Simulation. SPIIRAS Proceedings. 2018. Issue 4(59). 115 -139 / DOI 10.15622/sp.59.5
2. Biro M., Mashkoor A., Sametinger J., Seker R. Software Safety and Security Risk Mitigation in Cyber-physical Systems // IEEE Software. 2018. vol. 35. no. 1. pp. 24–29. DOI: 10.1109/MS.2017.4541050
3. Hu F. Cyber-Physical Systems: Integrated Computing and Engineering Design // New York: CRC Press. 2018. 398 p. ISBN 9781466577008
4. Eling M. What do we know about cyber risk and cyber risk insurance? // The Journal of Risk Finance. 2017. Iss. 5. P. 474–491. DOI: 10.1108/JRF-09-2016-0122
5. Subhayu Bandyopadhyay. The Economic Impact of Terrorism on Developing Countries. January 29, 2018
6. Subhayu Bandyopadhyay, Javed Younas. Trade and Terror: The Impact of Terrorism on Developing Countries. December 11, 2017
7. Bandyopadhyay, Subhayu; Sandler, Todd; and Younas, Javed. Foreign Direct Investment, Aid, and Terrorism. Oxford Economic Papers, January 2014, Vol. 66, No. 1, pp. 25-50.
8. James Andrew Lewis. The Economic Impact of Cybercrime— No Slowing Down. CSIS. February 21, 2018
9. Max Metzger. FBI says Ransomware soon becoming a billion dollar business. SC Media UK, January 10, 2017.
10. Arctic Potential: Realizing the Promise of U.S. Arctic Oil and Gas Resources. National Petroleum Council 2015.
11. World Energy Outlook 2017. OECD/IEA, September 14, 2017
12. World Energy Outlook 2018. The gold standard of energy analysis. OECD/IEA, 2018.
13. Лившиц И.И. Подходы к применению модели интегрированной системы менеджмента для проведения аудитов сложных промышленных объектов – аэропортовых комплексов // Труды СПИИРАН. 2014. Вып. 6. С. 72–94. ISSN 2078-9599
14. Лившиц И.И. Методика выполнения комплексных аудитов промышленных объектов для обеспечения эффективного внедрения систем энергоменеджмента // Энергобезопасность и энергосбережение. 2015. Вып. 3. С. 10-15.
15. Забайкин Ю.В., Заернюк В.М. Совершенствование механизма устойчивого развития промышленного предприятия: теория и методология. М.: Научные технологии, 2017. 263 стр. ISBN 978-5-4443-0116-6
16. Полетыкин А.Г. Формализованный метод оценки и управления рисками для обеспечения кибербезопасности больших систем управления / Материалы VIII Международной конференции «Управление развитием крупномасштабных систем» (MLSD'2015, Москва). — М.: ИПУ РАН, 2015. Т. I. С. 123–129. MLSD'2015
17. Заернюк В.М., Снитко Н.О. Оценка техногенных рисков в горнодобывающей отрасли // Известия высших учебных заведений // Геология и разведка. 2016. № 5. С. 73–78.
18. Ревенков П.В., Бердюгин А.А. Кибербезопасность в условиях Интернета вещей и электронного банкинга // Национальные интересы: приоритеты и безопасность. 2016. № 11 (344). С.158–169. ISSN 2311-875X
19. Плучевская Э.В., Овинникова К.Н. Актуальность процессного подхода при управлении проектами в нефтегазовой отрасли // Экономика и предпринимательство. 2014. 12-2 (53). С. 681-686. ISSN: 1999-2300
20. Рябов А.А. Проекты руководств по безопасности на опасных производственных объектах нефтегазового комплекса // Безопасность труда в промышленности. 2014. 12. С. 68-70.
21. Мастепанов А.М. Нефтегазовые проекты на арктическом шельфе в условиях высоких и низких цен на энергоресурсы // Научный журнал российского газового общества. 2016. 4. С.1-18. ISSN: 2412-6497
22. Ермолина Л.В., Ильина Л.А. Особенности управления проектами акселерации развития бизнеса нефтегазовых предприятий // Известия Волгоградского государственного технического университета. 2016. 16 (195). С. 80-84.

PRACTICE OF CYBER-RISKS MANAGEMENT IN OIL AND GAS PROJECTS OF HOLDING COMPANIES

Livshitz I.I.[19]

Abstract. *A significant part of the projects for the development of cyber risk management systems in oil and gas projects, either does not lead to the expected results, or in fact requires more resources than planned. One of the reasons for this situation seems to be the lack of reliable and practically tested risk management tools at the disposal of senior management and the project team, especially in the early stages of the life cycle. The presented publication will consider an example of a significant duration of the project for which the development of a risk management system was carried out.*

Purpose. *Analysis of existing approaches to cyber risk management and development of recommendations for information security in oil and gas projects of holding companies.*

Research methods. *Methods of system analysis and methods of theoretical and comparative analysis are used. The risks arising at various stages of preparation of oil and gas projects are investigated.*

19 I.I. Livshitz, Dr. Sc., professor ITMO University, St.-Petersburg, Russia, E-mail: Livshitz.il@yandex.ru

Results. *A system of identifying sources, identification and analysis of cyber risks that can affect the implementation of oil and gas projects for holding companies has been developed. The stages of the life cycle are considered and the need to ensure information security with the involvement of consulting companies is noted.*

It is recommended to pay attention to the degree of maturity of the consulting companies involved. Information security is proposed to be implemented at different levels: in assessing the competencies of specialists used it, culture analysis and preparation of reporting documents. The results of the study were applied in the implementation of oil and gas projects.

Keywords

Project, oil and gas project, risks, cyber risks, management system, integrated management system, information security, audit.

References

1. Teilans A.A., Romanovs A.V., Merkuryev Yu.A., Dorogovs P.P., Kleins A.Ya., Potryasaev S.A. / Assessment of Cyber Physical System Risks with Domain Specific Modelling and Simulation. SPIIRAS Proceedings. 2018. Issue 4(59). 115 -139 / DOI 10.15622/sp.59.5
2. Biro M., Mashkoor A., Sametinger J., Seker R. Software Safety and Security Risk Mitigation in Cyber-physical Systems // IEEE Software. 2018. vol. 35. no. 1. pp. 24–29. DOI: 10.1109/MS.2017.4541050
3. Hu F. Cyber-Physical Systems: Integrated Computing and Engineering Design // New York: CRC Press. 2018. 398 p.. ISBN 9781466577008
4. Eling M. What do we know about cyber risk and cyber risk insurance? // The Journal of Risk Finance. 2017. Iss. 5. P. 474–491. DOI: 10.1108/JRF-09-2016-0122
5. Subhayu Bandyopadhyay, The Economic Impact of Terrorism on Developing Countries. January 29, 2018
6. Subhayu Bandyopadhyay, Javed Younas. Trade and Terror: The Impact of Terrorism on Developing Countries. December 11, 2017
7. Bandyopadhyay, Subhayu; Sandler, Todd; and Younas, Javed. Foreign Direct Investment, Aid, and Terrorism. Oxford Economic Papers, January 2014, Vol. 66, No. 1, pp. 25-50.
8. James Andrew Lewis. The Economic Impact of Cybercrime — No Slowing Down. CSIS. February 21, 2018
9. Max Metzger. FBI says Ransomware soon becoming a billion dollar business. SC Media UK, January 10, 2017.
10. Arctic Potential: Realizing the Promise of U.S. Arctic Oil and Gas Resources. National Petroleum Council 2015.
11. World Energy Outlook 2017. OECD/IEA, September 14, 2017
12. World Energy Outlook 2018. The gold standard of energy analysis. OECD/IEA, 2018.
13. Livshits I. Podhodi k primeneniy modeli integrirovannoy sistemy memegzhmenta dly provedeniy auditov slozhnyh promishlennyh objectov – aeroportovyh kompleksov // Trydi SPIIRAN. 2014. 6. 72–94 pp.
14. Livshitz I. Metodika vypolneniy kompleksnyh auditov promishlennyh objectov dly obespechenia effectivnigo vnegrenia system energomenegzhmenta // Energobezopasnost' I Energosberezhenie. 2015. 3. 10-15 pp.
15. Zabaikin Y., Zaernyk V., Soversnenstvovanie mechanism usto'chivogo rezvitiya promyshlennogo predpriyatia. M.: Nauchnie technolii. 2017. 263 p.. ISBN 978-5-4443-0116-6
16. Poletikin A. Formalizovannyi' metod ocenki I upravleniya riskami dly obespechenia kiberbezopasnosti bol'shih system upravlenia/ Materialy VIII Mezdunarodno' konferencii "Upravlenie razvitiem krupnomashtabnih sistem" MLSD'2015, Moskva. M. IPU RAN. 2015. 1. 123-129 pp.. MLSD'2015
17. Zairnyk V., Snitko N. Ocenka technogennyh riskov v gornodobivayshei otrasly // Izvestia vysshih uchebnich zavedeni'. Geologia I razvedka. 2016. 5. 73-78 pp.
18. Revenkov P., Bergugin A. Kiberbezopasnost' v usloviyah internet veshe' I elektonnogo bankinga // Nacional'nie interesy: prioritety I bezopasnost'. 2016. 11 (344). 158-169 pp.. ISSN 2311-875X
19. Pluchevskay E., Ovinnikova K. Aktual'nost' processnogo podhoda pri upravlenii proektami v neftegazovoi otrasli // Ekonomika I predprinimatel'stvo. 2014. 12-2 (53). 681-686 pp.. ISSN: 1999-2300
20. Ryabov A. Proekti rukovodstva po bezopasnosti na opasnih proizvodstvennih ob'ektah neftegazovogo kompleksa // Bezopasnost' truda v promishlennosti. 2014. 12. 68-70 pp.
21. Mastepanov A. Neftegazovye proekty na arkticheskom shel'fe v usloviyah vysokih I nizkih cen na energoresursy // Nauchni' zhurnal rossi'skogo gazovogo obshestva. ISSN: 2412-6497. 2016. 4. 11-18 pp.. ISSN: 2412-6497
22. Ermolina L., Il'ina L. Osobennosti upravleniya proektami akseleracii razvitiy biznesa neftegazovih predpriyati' // Izvestiy Volgogradskogo gosudarstvennogo tehnicheskogo universiteta. 2016. 16 (195). 80-84 pp.