

Общество с ограниченной ответственностью
«Технологии знания»
ОГРН 1137746518161, ИНН 7721797593

УТВЕРЖДАЮ

Генеральный директор
ООО «Технологии знания»
Колесникова М.С.



01 августа 2026 г.

**Дополнительная профессиональная программа повышения
квалификации «VAP: Управление рисками в ИТ»**

г. Москва, 2026

Цель программы: Получение новых знаний и навыков, повышение квалификации специалистов и руководителей подразделений ИТ (информационных технологий), в связи с повышением требований к уровню квалификации и необходимостью освоению современных методов решения профессиональных задач.

Задачи программы:

- Дать слушателям системное понимание управления ИТ-рисками как инструмента поддержки управленческих решений и снижения неопределённости.
- Научить выявлять, корректно описывать, оценивать и приоритизировать ИТ-риски с учётом их вероятности, последствий и финансовых показателей.
- Научить выбирать и обосновывать меры реагирования на риски, оценивать их стоимость и определять величину остаточного риска.
- Помочь слушателям выстроить управление ИТ-рисками и встроить его в существующие процессы управления ИТ-услугами, проектами и операционной деятельностью.
- Дать слушателям практические инструменты для организации работы с ИТ-рисками, включая структуру реестра ИТ-рисков, адаптированную к особенностям ИТ-организации.
- Сформировать понимание ролей и ответственности участников управления рисками, а также принципов организации управленческого контура риск-менеджмента.

Что получают слушатели:

- Знания и практические навыки, необходимые для системного управления ИТ-рисками.
- Понимание того, как использовать информацию о рисках для планирования и принятия управленческих решений.
- Методики выявления, описания, оценки и приоритизации ИТ-рисков, включая методы количественной и финансовой оценки.
- Практические подходы к выбору мер реагирования на риски и оценке их эффективности.
- Понимание того, как встроить управление рисками в управление ИТ-услугами, проектами и операционную деятельность.
- Практический инструмент — структуру реестра ИТ-рисков, адаптированную для использования в ИТ-организации.

Категория слушателей: к освоению программы допускаются лица, имеющие высшее либо среднее профессиональное образование.

Срок обучения: 19 часов.

Форма обучения: дистанционная (обучение с применением дистанционных образовательных технологий), очная

Режим обучения: определяется совместно с Заказчиком.

После освоения программы слушатель должен

знать:

- основные принципы управления ИТ-рисками: назначение риск-менеджмента, его связь с управлением бизнес-рисками, особенности ИТ-рисков и основные стандарты и рекомендации по управлению рисками.
- принципы корректного описания ИТ-рисков: причины, риск, последствия и взаимосвязь между ними; отличие риска от проблемы (issue).
- методы оценки и приоритизации ИТ-рисков: качественные и количественные подходы к оценке влияния и вероятности, рейтинг риска, взвешенную стоимость риска и оценку в финансовых показателях.
- основные подходы к реагированию на риски: принятие, снижение, перенос и избегание; принципы оценки стоимости мер реагирования и остаточного риска.
- подходы к категоризации и структурированию ИТ-рисков, включая классификацию по источникам и последствиям, а также дополнительные атрибуты риска.
- принципы построения управленческого контура управления ИТ-рисками: политики и правила, риск-аппетит, уровни принятия решений, точки контроля и пересмотра рисков.
- особенности управления рисками в ИТ-услугах и ИТ-проектах, а также взаимосвязь управления рисками с другими ИТ-практиками.
- основные роли и зоны ответственности участников управления ИТ-рисками.
- методы выявления и анализа ИТ-рисков: интервьюирование, анализ статистики, метод Монте-Карло, мозговой штурм, метод Делфи, «5 почему», дерево решений и дерево рисков.
- основные возможности, ограничения и принципы автоматизации управления ИТ-рисками.

уметь:

- выявлять и корректно описывать ИТ-риски, выделяя причины, риск и возможные последствия.
- оценивать вероятность и влияние ИТ-рисков с использованием качественных и количественных методов.
- приоритизировать ИТ-риски и сопоставлять их между собой на основе степени влияния, вероятности и финансовых показателей.
- выбирать стратегию реагирования на риск, оценивать стоимость мер реагирования и определять остаточный риск.
- разрабатывать и структурировать реестр ИТ-рисков с учётом особенностей ИТ-организации.
- выстраивать управление ИТ-рисками на разных уровнях принятия решений — от уровня организации до уровня услуги, проекта и операционной деятельности.
- встраивать управление рисками в процессы управления ИТ-услугами, проектами, изменениями, проблемами, SLA, проектирования услуг и управления финансами ИТ.

- определять роли и ответственность участников управления ИТ-рисками.
- выбирать подходящие методы выявления и анализа рисков в зависимости от поставленной задачи и имеющихся данных.
- определять целесообразность автоматизации управления ИТ-рисками и требования к инструментам автоматизации.

владеть навыками:

- выявления и корректного описания ИТ-рисков.
- качественной и количественной оценки ИТ-рисков.
- оценки рисков в финансовых показателях и определения взвешенной стоимости риска.
- приоритизации ИТ-рисков.
- выбора и обоснования стратегии реагирования на ИТ-риски.
- оценки стоимости мер реагирования и остаточного риска.
- категоризации и структурирования ИТ-рисков.
- разработки и ведения реестра ИТ-рисков.
- интеграции управления рисками с другими ИТ-практиками и процессами.
- применения методов выявления и анализа ИТ-рисков.
- использования информации о рисках для поддержки управленческих решений.
- определения подходов к автоматизации управления ИТ-рисками.

№ п/п	Наименование разделов и дисциплин	Всего	Количество часов по видам занятий		Форма аттестации и контроля знаний
			Лекции	Практика	
			4	5	
1	2	3	4	5	6
1	Краткое введение в управление ИТ-рисками. Зачем управлять рисками в ИТ и какую управленческую задачу это решает. Связь управления ИТ-рисками и управления бизнес-рисками. Что происходит, если рисками не управлять. Особенности рисков в ИТ. О каких рисках может идти речь? Обзор стандартов и рекомендаций по управлению рисками.	1	1	0	
2	Понятие риска и корректное описание ИТ-рисков. Что такое риск и чем он отличается от проблемы (issue). Атрибуты риска: причина, риск, последствие и их взаимосвязь. Примеры корректно и некорректно описанных рисков. Упражнение: выявление и описание рисков по предложенному кейсу.затраты,	2	1	1	

	методы отнесения затрат. Постоянные и переменные затраты, значащий интервал. Упражнение. Классификация затрат. Обсуждение. База распределения косвенных затрат.				
3	Оценка и приоритизация ИТ-рисков. Подходы к оценке влияния риска: качественные и количественные. Подходы к оценке вероятности риска. Рейтинг риска как функция влияния и вероятности. Взвешенная стоимость риска и оценка в финансовых показателях. Источники данных для оценки рисков. Упражнение: оценка и приоритизация рисков по предложенному кейсу.	2	1	1	
4	Реагирование на риски и повторная оценка. Подходы к работе с рисками: принятие, снижение, перенос, избегание. Стоимость мер реагирования и их сопоставление с величиной риска. Остаточный риск и повторная оценка. Упражнение: выбор стратегии реагирования и оценка остаточного риска.	2	1	1	
5	Категоризация и структурирование ИТ-рисков. Подходы к категоризации рисков по источникам и последствиям. Риски ИТ-организации и риски заказчика. Уверенность в полноте категоризации: 4 аспекта управления услугами, ТЕСОР, варианты кастомизированных подходов. Дополнительные атрибуты риска: степень приближения (Cost of Delay), место возникновения и прочие. Упражнение: финализация структуры реестра ИТ-рисков.	2	1	1	
6	Управленческий контур управления ИТ-рисками. Политики и правила управления ИТ-рисками. Риск-аппетит и склонность к рискам, связь с этапом развития организации. Управление рисками на разных уровнях принятия решений: риски уровня организации, риски услуги/проекта, операционные риски. Управление рисками в ИТ-услугах и ИТ-проектах: сходства и различия. Управление рисками и жизненный цикл услуги. Процесс управления рисками на фазе эксплуатации и точки контроля и	3	2	1	

	пересмотра рисков. Дискуссия: метрики управления ИТ-рисками.				
7	Связь управления рисками с другими ИТ-практиками. Упражнение: проработка связей управления рисками с другими практиками. Взаимосвязь с управлением проблемами, изменениями и SLA, проектированием услуг и управлением финансами ИТ.	2	1	1	
8	Роли и ответственность в управлении рисками. Роль менеджера рисков. Участие других ролей организации в управлении рисками. Командная работа.	1	1	0	
9	Методы выявления и анализа ИТ-рисков. Интервьюирование. Анализ статистики и метод Монте-Карло. Мозговой штурм. Метод Делфи. «5 почему». Дерево решений. Дерево рисков. Комбинирование методов.	1	1	0	
10	Автоматизация в управлении рисками (обзорно). Целесообразность и ограничения автоматизации управления рисками. Основные и достаточные характеристики инструментов автоматизации. Рекомендации по автоматизации управления рисками.	2	2	0	
11	Рекомендации и подведение итогов. Типовые сложности и способы их решения. Подведение итогов курса.	1	1	0	
	Всего часов:	19	13	6	
	Итоговая аттестация	зачет			

Содержание тем дополнительной профессиональной программы повышения квалификации.

Тема 1. Краткое введение в управление ИТ-рисками. Зачем управлять рисками в ИТ и какую управленческую задачу это решает. Связь управления ИТ-рисками и управления бизнес-рисками. Что происходит, если рисками не управлять. Особенности рисков в ИТ. О каких рисках может идти речь? Обзор стандартов и рекомендаций по управлению рисками.

Тема 2. Понятие риска и корректное описание ИТ-рисков. Что такое риск и чем он отличается от проблемы (issue). Атрибуты риска: причина, риск, последствие и их взаимосвязь. Примеры корректно и некорректно описанных рисков. Упражнение: выявление и описание рисков по предложенному кейсу.

Тема 3. Оценка и приоритизация ИТ-рисков. Подходы к оценке влияния риска: качественные и количественные. Подходы к оценке вероятности риска. Рейтинг риска как

функция влияния и вероятности. Взвешенная стоимость риска и оценка в финансовых показателях. Источники данных для оценки рисков. Упражнение: оценка и приоритизация рисков по предложенному кейсу.

Тема 4. Реагирование на риски и повторная оценка. Подходы к работе с рисками: принятие, снижение, перенос, избегание. Стоимость мер реагирования и их сопоставление с величиной риска. Остаточный риск и повторная оценка. Упражнение: выбор стратегии реагирования и оценка остаточного риска.

Тема 5. Категоризация и структурирование ИТ-рисков. Подходы к категоризации рисков по источникам и последствиям. Риски ИТ-организации и риски заказчика. Уверенность в полноте категоризации: 4 аспекта управления услугами, ТЕСОР, варианты кастомизированных подходов. Дополнительные атрибуты риска: степень приближения (Cost of Delay), место возникновения и прочие. Упражнение: финализация структуры реестра ИТ-рисков.

Тема 6. Управленческий контур управления ИТ-рисками. Политики и правила управления ИТ-рисками. Риск-аппетит и склонность к рискам, связь с этапом развития организации. Управление рисками на разных уровнях принятия решений: риски уровня организации, риски услуги/проекта, операционные риски. Управление рисками в ИТ-услугах и ИТ-проектах: сходства и различия. Управление рисками и жизненный цикл услуги. Процесс управления рисками на фазе эксплуатации и точки контроля и пересмотра рисков. Дискуссия: метрики управления ИТ-рисками.

Тема 7. Связь управления рисками с другими ИТ-практиками. Упражнение: проработка связей управления рисками с другими практиками. Взаимосвязь с управлением проблемами, изменениями и SLA, проектированием услуг и управлением финансами ИТ.

Тема 8. Роли и ответственность в управлении рисками. Роль менеджера рисков. Участие других ролей организации в управлении рисками. Командная работа.

Тема 9. Методы выявления и анализа ИТ-рисков. Интервьюирование. Анализ статистики и метод Монте-Карло. Мозговой штурм. Метод Делфи. «5 почему». Дерево решений. Дерево рисков. Комбинирование методов.

Тема 10. Автоматизация в управлении рисками (обзорно). Целесообразность и ограничения автоматизации управления рисками. Основные и достаточные характеристики инструментов автоматизации. Рекомендации по автоматизации управления рисками.

Тема 11. Рекомендации и подведение итогов. Типовые сложности и способы их решения. Подведение итогов курса.