

Контрольная работа № 1			
№ п/п	Вопрос	Варианты ответов	Код
1	аудит безопасности системы информационных технологий — это	систематический, независимый и документированный процесс получения свидетельств аудита и объективного их оценивания с целью установления степени выполнения требований по обеспечению состояния защищенности системы информационных технологий	А
		системный процесс получения объективных качественных и количественных оценок о текущем состоянии ИБ компании в соответствии с определенными критериями и показателями безопасности	Б
		периодический, независимый от объекта аудита и документированный процесс получения свидетельств аудита и объективной их оценки с целью установления степени выполнения в организациях установленных требований по обеспечению ИБ	В
		проверка используемых компанией информационных систем, систем безопасности, систем связи с внешней средой, корпоративной сети на предмет их соответствия бизнес-процессам, протекающим в компании, а также соответствия международным стандартам, с последующей оценкой рисков сбоев в их функционировании.	Г
2	Какие методологические подходы к решению проблемы доверия к мерам ИБ используются в настоящее время?	Получение свидетельств доверия к объекту путем его испытания, т.е. практического подтверждения убежденности в том, что объект обладает ожидаемыми свойствами	А
		Получение свидетельств доверия к объекту путем изучения документации, регламентирующей его деятельность	Б
		Получение свидетельств доверия к объекту путем получения необходимых сертификатов и лицензий	В
		Получение свидетельств доверия (уверенности) в том, что некая деятельность, от которой зависит эффективность работы самого объекта, осуществляется правильно.	Г
3	Оценка эффективности деятельности или качества изделия в обязательном порядке требует:	Выбора ключевых показателей (индикаторов), характеризующих количественное или качественное состояние свойств объекта или какой-либо деятельности	А
		Выбора метода измерения выбранных ключевых показателей и оценки его точности	Б
		Определения критериев оценки соответствия измеренных показателей установленным требованиям, характеризующим приемлемый с точки зрения владельца объекта уровень его качества или качества аудируемой деятельности	В
		Получения гарантий оценки	Г
4	Что не относится к целям аудита информационной безопасности?	Внедрение и тестирование средств защиты информации в организации	А
		Разработка и внедрение политик информационной безопасности в организации	Б
		Оценка текущего состояния информационной безопасности организации в соответствии с разработанной моделью угроз	В
		Проверка состояния защищенности конфиденциальной информации в организации, а также программного и аппаратного обеспечения, от которого зависит бесперебойное функционирование системы информационных технологий	Г
5	Важными факторами для успешной оценки процесса являются:	Определение целей и задач аудита	А
		Доверие	Б
		Осознание и мотивация руководства организации	В
		Наличие необходимых методик проведения аудита	Г
6	Аудит второй стороны	это аудит, выполняемый внешней независимой организацией.	А
		это аудит, при котором заказчиком аудита является не сама проверяемая организация, а ее клиент.	Б
		это внутренний аудит, при котором организация проверяет сама себя.	В
		это внешний аудит, заказчиком которого является сама организация	Г
7	Суть экспертного аудита информационной безопасности заключается в	определении степени соответствия выбранным стандартам и внутренним требованиям организации в области информационной безопасности	А
		исследовании системы обеспечения информационной безопасности организации и в ее сравнении с некоторой идеальной системой обеспечения информационной безопасности	Б
		определении актуальных угроз информационной безопасности и построении модели угроз информационной безопасности	В
		проведении экспертами настоящих атак на информационную систему заказчика, это исследование состояния защищенности информационной системы	Г