Общество с ограниченной ответственностью «АТЭК-С»
(ООО «АТЭК-С»)
350080, Россия, Краснодарский край, г. Краснодар, тер. Пашковский жилой массив, ул. Заводская, д. 32, оф. 203
тел./факс: (861) 266-73-03, 266-28-67, 266-28-68
www.atekgc.ru, e-mail: office@atekgc.ru
ОКПО 97754875; ОГРН 1062312041296;
ИНН/КПП 2312133345 / 231201001

УТВЕРЖДАЮ
Директор ООО «АТЭК-С»

_____ Косяков Е.В.
(подпись)

«01» сентября 2025 года

УЧЕБНЫЙ ПЛАН
дополнительной программы повышения квалификации

«Обеспечение информационной безопасности в органах государственной власти»

Цель обучения: Целью реализации дополнительной профессиональной программы является обучение специалистов по информационной безопасности современным рискам информационной безопасности, практическим принципам обеспечения защиты данных, мерам по повышению эффективности государственных структур для противодействия киберпреступлениям. Область профессиональной деятельности слушателя, освоившего программу повышения квалификации, включает выполнение работ по противодействию рискам информационной безопасности в органах государственной власти.
Категория слушателей: Государственные гражданские служащие.
Требования к квалификации поступающих на обучение: лица, имеющие среднее профессиональное и (или) высшее образование
Срок обучения: 40 (сорок) академических часов
Форма обучения: очная, с применением дистанционных технологий

Наименование разделов и тем	Всего часов	В том числе, час				
		Л	СЗ	ПЗ	Зач	К, СР
1	2	3	4	5	6	7
Входное тестирование	1				1	
Раздел 1. Комплексный подход к защите от инсайдерских угроз: практика предотвращения инцидентов	14	6		8		
Тема 1: Актуальные данные по утечкам данных в государственных органах	1	1				

Наименование разделов и тем	Всего часов	В том числе, час				
		Л	СЗ	ПЗ	Зач	К, СР
1	**2**	**3**	**4**	**5**	**6**	**7**
Тема 2: Стратегии и мотивы инсайдеров	1	1				
Тема 3: Риски ИБ: утечки данных, саботаж, внешние и внутренние атаки и другие	4	2		2		
Тема 4: Кейсы расследований	2			2		
Тема 5: Виды социальной инженерии: фишинг, «дорожное яблоко», троянский конь и другие	4	2		2		
Тема 6: Что делать, чтобы уменьшить влияние социальной инженерии	2			2		
Раздел 2.Системы защиты информации.	**24**	**11**		**13**		
Тема 1: Уязвимости и способы их устранения	3	1		2		
Тема 2: Виды компьютерных инцидентов и объекты воздействия	4	2		2		
Тема 3: Стратегия защиты информации	2	1		1		
Тема 4: Уровни защиты данных	2	2		-		
Тема 5: Средства защиты информации, практика применения	3	1		2		
Тема 6: Дополнительные способы защиты: шифрования, метки и другие	3	1		2		
Тема 7: Группы риска: сотрудники, которые чаще всего становятся виновниками инцидентов	3	1		2		
Тема 8: Государственные регуляторы в сфере ИБ	2	2		-		
Тема 9: Обзор судебной практики по делам, связанным с нарушениями в области ИБ	2	-		2		
Итоговая аттестация (тестирование)	**1**				1	
Итого	**40**	**17**		**21**	**2**	