

АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Поспелов Евгений
Менеджер по продажам решений ИБ



Цели и виды аттестации объектов информатизации

Аттестация объектов информатизации (ОИ) – комплекс организационно-технических мероприятий, в результате которых подтверждается соответствие системы защиты информации объекта информатизации требованиям безопасности информации.

Обязательной аттестации подлежат:

1. обрабатывающие ГТ;
2. помещения для ведения секретных переговоров;
3. ГИС;
4. ИС, подключаемые к информационным ресурсам ГК Ростех, ГК Росатом, ГИС

Необязательной аттестации подлежат:

1. ИСПДн;
2. ОКИИ
3. АСУ ТП

Целью проведения аттестации:

является подтверждение соответствия системы защиты информации в реальных условиях эксплуатации требованиям безопасности информации.

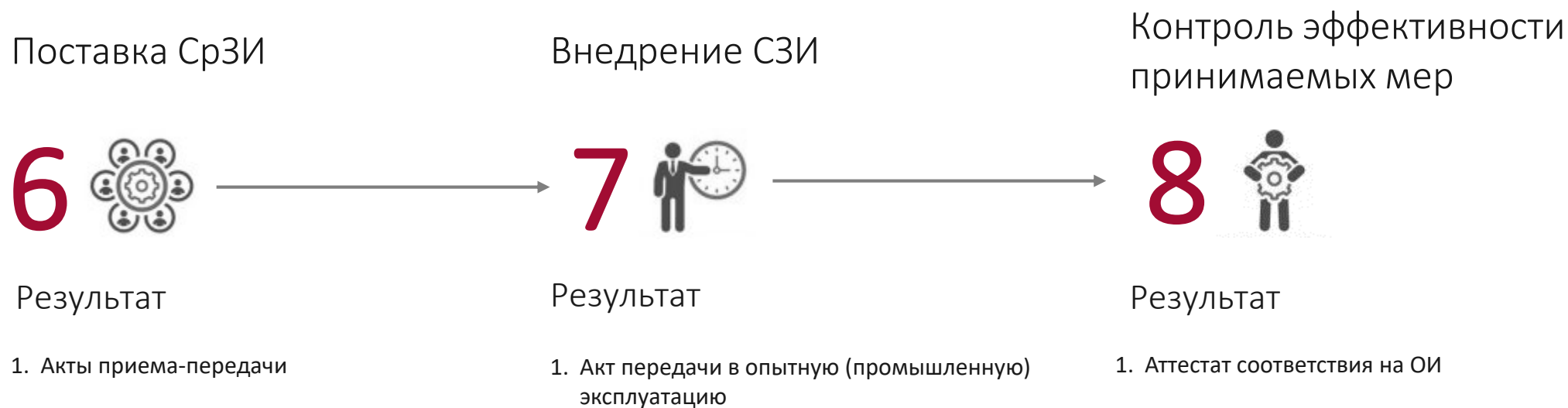
Проведение комплекса работ по аттестации



Первый блок работ по аттестации



Второй блок работ по аттестации



Изменения в Положении по аттестации ОИ

Требование	Было	Стало
Аттестат соответствия выдается	ГИС - на весь срок эксплуатации, для остальных ОИ на 3 года	на весь срок эксплуатации объекта информатизации
Направление во ФСТЭК аттестационных документов по окончании выполнения работ**	-	в течение 5 рабочих дней со дня подписания аттестата
Проведения периодического контроля уровня защиты информации на аттестованном объекте информатизации	С разной периодичностью, отправлять во ФСТЭК России ничего не нужно	Протоколы контроля защиты информации на аттестованном ОИ не реже одного раза в два года представляются владельцем ОИ в ФСТЭК России*

* Непредставление протоколов контроля защиты информации в ФСТЭК России (территориальный орган ФСТЭК России) является основанием для приостановления действия аттестата соответствия.

** Невозможность внести измен

Важно при работе с ЦОД

Серверный сегмент:

1. Сервера расположенные на территории ЦОД и не только.

2. ЦОД аттестован до виртуализации.

Пользовательский сегмент:

1. АРМы пользователей оператора ОИ.

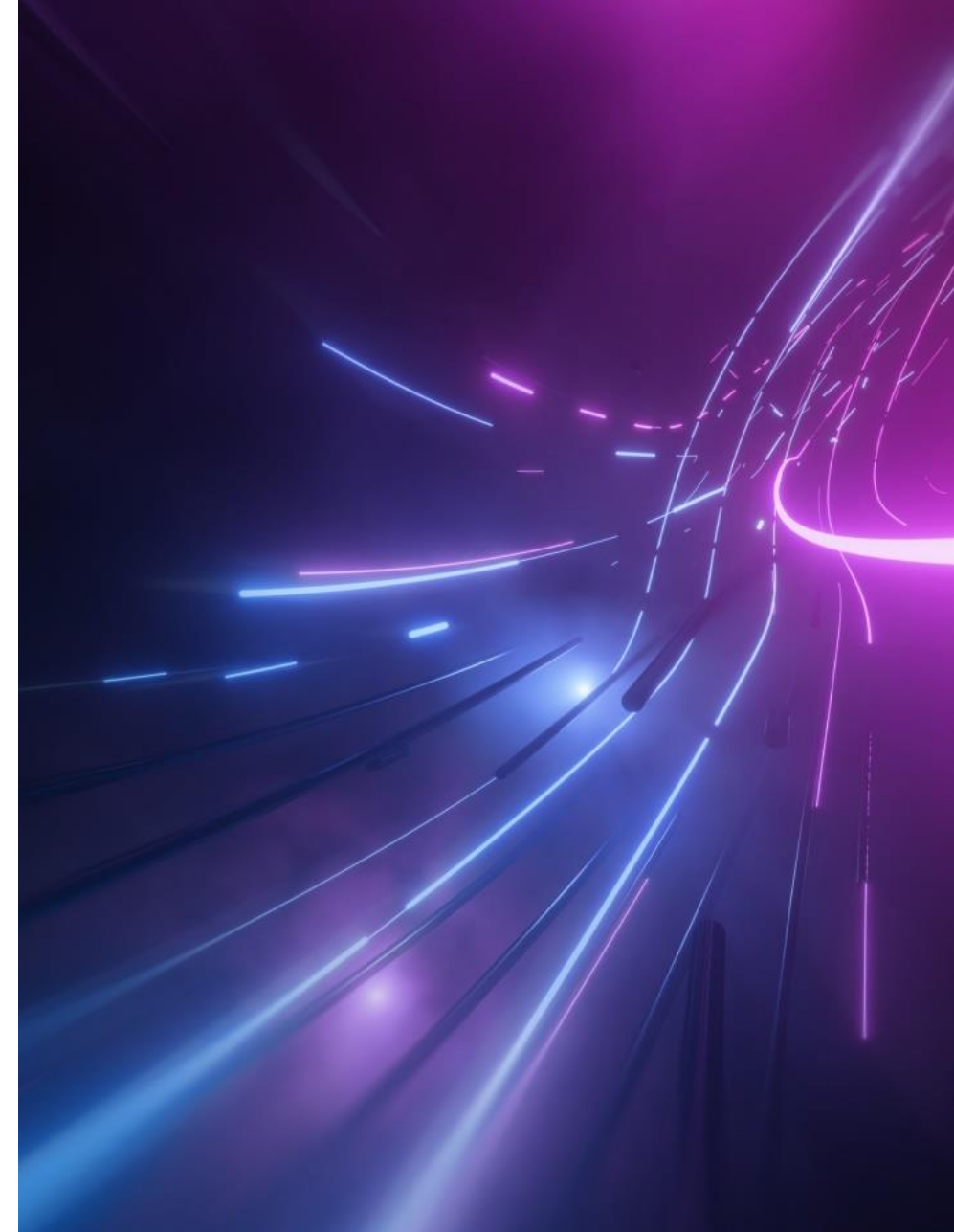
2. Необходимо внедрять СЗИ

Типовые СрЗИ

СЗИ	АС	ИСПДн				ГИС			Основной вариант	Альтернативный
	1Г	УЗ-4	УЗ-3	УЗ-2	УЗ-1	К3	К2	К1		
АВЗ	+	+	+	+	+	+	+	+	Kaspersky Endpoint Security	Dr. Web
НСД	+	+	+	+	+	+	+	+	SNS (модуль НСД)	Dallas Lock 8.0-К
СКН	+			+	+	+	+	+	SNS (контроль устройств)	Dallas Lock 8.0-К
АНЗ			+	+	+	+	+	+	xSpider 7.8, MaxPatrol	Сканер-ВС
МДЗ				+	+		+	+	ПАК «Соболь» 3.0	СДЗ «Dallas Lock»
СОВ				+	+		+	+	АПКШ «Континент», Secret Net Studio (модуль СОВ)	Dallas Lock 8.0-К
МЭ и СКЗИ	+	+	+	+	+	+	+	+	АПКШ «Континент», Континент-АП	VipNet Coordinator
ЗСВ	+	+	+	+	+	+	+	+	vGate R2	VMware vSphere

Почему мы?

- Единая точка входа по любым задачам
 - Работаем с 99% вендоров
- Профессионалы своего дела
 - Выполняем работы собственной командой консультантов и инженеров с высшим образованием по ИБ, а также с сертификатами: CISA, CISM, PMP, ISO 27001.
- Большой опыт
 - Более 100 выполненных проектов
- Лицензиаты
 - Являемся лицензиатами ФСТЭК и ФСБ России.



Q&A

softline[®] 

Цифровая Трансформация.
Успешная. Эффективная.