

УТВЕРЖДАЮ
Директор ФСТЭК России

В.Селин

11 августа 2026 г.

ПЕРЕЧЕНЬ
КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНОГО И ИСПЫТАТЕЛЬНОГО ОБОРУДОВАНИЯ, ПРОГРАММНЫХ (ПРОГРАММНО-ТЕХНИЧЕСКИХ) СРЕДСТВ, НЕОБХОДИМЫХ ДЛЯ ВЫПОЛНЕНИЯ РАБОТ И ОКАЗАНИЯ УСЛУГ,
УСТАНОВЛЕННЫХ ПОЛОЖЕНИЕМ О ЛИЦЕНЗИРОВАНИИ ДЕЯТЕЛЬНОСТИ
ПО РАЗРАБОТКЕ И ПРОИЗВОДСТВУ СРЕДСТВ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ,
УТВЕРЖДЕННЫМ ПОСТАНОВЛЕНИЕМ
ПРАВИТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ОТ 3 МАРТА 2012 Г. № 171

№ п/п	Наименование оборудования, программных (программно- технических) средств	Технические и (или) функциональные характеристики	Виды работ и (или) услуг по разработке и производству СЗКИ*											
			а) разработка						б) производство					
			a1	a2	a3	a4	a5	a6	б1	б2	б3	б4	б5	б6
			технических средств защиты информации	защищенных технических средств обработки информации	технических средств контроля эффективности мер защиты информации	программных (программно-технических) средств защиты информации	защищенных программных (программно-технических) средств обработки информации	программных (программно-технических) средств контроля защищенности информации	технических средств защиты информации	защищенных технических средств обработки информации	технических средств контроля эффективности мер защиты информации	программных (программно-технических) средств защиты информации	защищенных программных (программно-технических) средств обработки информации	программных (программно-технических) средств контроля защищенности информации
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Генератор низкочастотных	Диапазон рабочих частот 175...5600 Гц.	+	+	+				+	+	+			

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	сигналов (при необходимости с усилителем)	Уровень мощности выходного сигнала не менее 25 дБм												
2	Акустический излучатель	Диапазон рабочих частот: 175...5600 Гц. Интегральный уровень звукового давления на расстоянии 1 м по оси излучения не менее 94 дБ. Неравномерность АЧХ не более ± 6 дБ. Нестабильность уровня интегрального звукового давления в течение непрерывной работы не более ± 2 дБ	+	+	+				+	+	+			
3	Измерительный микрофон	Диапазон рабочих частот: 175...5600 Гц. Чувствительность не менее 10 мВ/Па. Неравномерность АЧХ не более ± 2 дБ Наличие свидетельства о поверке	+	+	+				+	+	+			
4	Датчики виброускорения (акселерометры)	Диапазон рабочих частот: 175...5600 Гц. Чувствительность не менее 10 мВ/мс ⁻² . Нелинейность амплитудной характеристики не более ± 10 %. Масса не более 30 г. Наличие свидетельства о поверке	+	+	+				+	+	+			
5	Селективные микровольтметры	Диапазон рабочих частот: 175...5600 Гц. Погрешность измерения не более ± 20 %. Наличие свидетельства о поверке	+	+	+				+	+	+			
6	Вольтметр (мультиметр)	Диапазон рабочих частот: 175-5600 Гц. Погрешность измерения напряжения не более ± 15 %	+	+	+				+	+	+			
7	Лабораторный автотрансформатор	Диапазон регулировки напряжения: 0...270 В	+	+	+				+	+	+			
8	Датчик переменной силы (с усилителем)	Диапазон частот: 175...5600 Гц Чувствительность: не менее 1 пКл/Н. Неравномерность АЧХ: не более 10%. Наличие свидетельства о калибровке	+	+	+				+	+	+			
9	Динамометрический ключ	Диапазон измерения момента затяжки: 1-3 Н*м	+	+	+				+	+	+			

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
10	Массивная нагрузка	Металлическая нагрузка массой не менее 5 кг	+	+	+				+	+	+			
11	Осциллограф	Диапазон измеряемых параметров 0...5 МГц	+	+	+				+	+	+			
12	Помещение для акустических измерений	Объем помещения не менее 40 м ³ . Октавные уровни фоновых акустических шумов помещения не более 40 дБ/2*10 ⁻⁵ Па в октавных полосах со среднегеометрическими частотами 250, 500 Гц; не более 35 дБ/2*10 ⁻⁵ Па в октавных полосах со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц. На помещения должен быть оформлен протокол измерения акустических шумов	+	+	+				+	+	+			
13	Рефлектометры (микрорефлектометры)	Длина волны калибровки: 850, 1300, 1550 нм. Диапазон измерений оптической мощности: от 3 до минус 26 – минус 65 дБм. Длительность импульса от 10 до 20000 нс. Наличие свидетельства о поверке	+	+	+				+	+	+			
14	Оптические тестеры (измерители мощности)	Длина волны калибровки: 850, 1310, 1550 нм. Диапазон измерений оптической мощности: от 3 до минус 10 - минус 73 дБм. Разрешающая способность: 0,1 ... 0,001 дБ. Наличие свидетельства о поверке	+	+	+				+	+	+			
15	Комплект оптических аттенюаторов и нагрузок	Длина волны калибровки: 850, 1300, 1310, 1550 нм. Диапазон измерений ослабления оптического излучения: 0...80 дБ. Погрешность измерений ослабления: ±0,5 дБ. Наличие свидетельства о поверке	+	+	+				+	+	+			
16	Средство поиска остаточной информации на машинных носителях информации	Обеспечение поиска остаточной информации на машинных носителях информации по заданным критериям. Наличие сертификата соответствия ФСТЭК России требованиям по безопасности информации				+	+	+				+	+	+

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
17	Средство (средства) контроля целостности программ и программных комплексов	Обеспечение расчета уникальных значений контрольных сумм программного обеспечения, а также документирование результатов расчета контрольных сумм. Обеспечение расчета контрольных сумм программного обеспечения, средой функционирования которого являются операционные системы Windows и Linux (допускается выполнять средствами сертифицированных операционных систем). Обеспечение расчета контрольных сумм программного обеспечения по алгоритму, установленному ГОСТ Р 34.11. Наличие сертификата соответствия ФСТЭК России требованиям по безопасности информации				+	+	+				+	+	+
18	Средства (системы) контроля (анализа) защищенности информационных систем (сканер безопасности)	Обнаружение (сканирование) сетевых портов (устройств в вычислительной сети). Определение топологии сети. Определение активных сетевых служб вычислительной сети, определение названий и версий программного обеспечения, обеспечивающих функционирование таких служб. Обеспечение поиска уязвимостей вычислительной сети, в том числе уязвимостей конфигурации вычислительной сети, уязвимостей программного обеспечения, функционирующего с применением операционных систем семейства Windows и Unix/Linux. Осуществление взаимодействия с банком данных угроз безопасности информации ФСТЭК России. Наличие сертификата соответствия ФСТЭК России требованиям по безопасности информации				+	+	+				+	+	+
19	Комплексы для тестирования на проникновение	Возможность выявления и эксплуатации в автоматизированном режиме различных уязвимостей кода, архитектуры и конфигураций программного обеспечения, в том числе связанных с:				+	+	+				+	+	+

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		различными правами доступа к файлам, устройствам, процессам и службам; избыточными правами (разрешениями) контейнеров и групп контейнеров; ошибками безопасного конфигурирования типовых программных компонент и другими												
20	Анализаторы сетевых протоколов	Перехват сетевого трафика, передаваемого по каналам связи и обрабатываемого на узле с исследуемым программным обеспечением. Анализ сетевого трафика на всех уровнях базовой эталонной модели взаимосвязи открытых систем, установленной ГОСТ Р ИСО/МЭК 7498-1. Фильтрация сетевого трафика с целью выявления в сетевом трафике сетевых пакетов, относящегося к исследуемому программному обеспечению. Возможность формирования правил анализа сетевых протоколов				+	+	+				+	+	+
21	Средство (средства) анализа исходных кодов программ (статический анализатор)	Обеспечение решения задач контроля отсутствия в программном обеспечении, разработанном на основных языках промышленного программирования C/C++, C#, JavaScript, Python, Perl, PHP, Go, недеklarированных возможностей. Обеспечение проведения статического анализа исходных кодов на уровне проведения синтаксического анализа кода программного обеспечения, а также контроля соответствия его объектному (загрузочному) коду. Обеспечение проведения контекстно-чувствительного и чувствительного к путям выполнения анализа исходного кода программного обеспечения. Статический анализатор (анализаторы) должны соответствовать требованиям Методики выявления уязвимостей и недеklarированных возможностей в программном обеспечении, утвержденной				+	+	+				+	+	+

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		ФСТЭК России 16 мая 2026 г. и национального стандарта ГОСТ Р 71207-2024												
22	Отладчик	Обеспечение возможности исследования программного кода в процессе выполнения программного обеспечения с использованием трассировки, отслеживания, установки или изменения значений переменных, установки и удаления контрольных точек или условий установки. Возможность интеграции с интегрированными средами разработки, эмуляторами и со средствами анализа бинарного кода (дизассемблерами и декомпиляторами) и инструментами анализа трасс				+	+	+				+	+	+
23	Средства разработки программ	Должны обеспечивать разработку, компиляцию и отладку программ, просмотр и редактирование бинарных файлов, разработку программ с возможностями подключения и расширения для программирования на различных языках, поиск фрагментов данных, сравнение фрагментов данных, расчет контрольных сумм фрагментов данных, проведение вычислений в системах счисления по десятичному, двоичному и шестнадцатеричному основаниям				+	+	+				+	+	+
24	Монитор активности приложений	Получение характеристик исследуемой программы под управлением операционных систем семейства Windows и Unix/Linux во время ее работы, в том числе: объем и диапазоны потребляемых ресурсов (память среды функционирования и другие); события взаимодействия со средой функционирования, в том числе системные вызовы (если применимо); события взаимодействия с файлами и устройствами хранения данных; события взаимодействия с сетевыми объектами и устройствами				+	+	+				+	+	+

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
25	Средства антивирусной защиты (не менее 2 средств разных производителей)	Обеспечение поиска вредоносного программного обеспечения в программных комплексах и в информационных системах, функционирующих с применением операционных систем семейства Windows и Unix/Linux. Наличие сертификата соответствия ФСТЭК России требованиям по безопасности информации				+	+	+				+	+	+
26	Компилятор	Компиляция программ, написанных на языках промышленного программирования (C/C++, C#, JavaScript, Python, Perl, PHP, Go)				+	+	+				+	+	+
27	Эмулятор	Имитирование работы аппаратных средств вычислительной техники путем приема, обработки и выдачи тех же входных и выходных данных, что используются имитируемым средством, запуск программ на платформах, для которых они не предназначены. Эмуляция основных архитектур общего назначения: x86-64, ARM, PowerPC, MIPS, RISC-V. При эмуляции процессорной архитектуры x86-64 должна обеспечиваться возможность применения технологий аппаратной виртуализации				+	+	+				+	+	+
28	Фаззер	Тестирование исследуемых программ путем передачи им наборов входных данных (сгенерированных случайным образом или по специальному шаблону). Фиксирование нарушения штатного функционирования программного обеспечения в результате обработки таких наборов входных данных. Инструментирование исходного или исполняемого кода программного обеспечения для обеспечения возможности генетического фаззинга. Анализ текстового покрытия кода программного обеспечения на уровне функциональных объектов и базовых блоков.				+	+	+				+	+	+

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		Применение метода символьного выполнения при формировании наборов входных данных и анализе нарушения штатного функционирования программы в результате обработки такого набора данных. Фаззер должен обеспечивать реализацию положений Методики выявления уязвимостей и недекларированных возможностей в программном обеспечении, утвержденной ФСТЭК России 16 мая 2026 г.												
29	Программатор	Чтение/запись данных в энергозависимую память устройства (PROM, EPROM, EEPROM, NVRAM, Флеш-память, 3D XPoint, FRAM, MRAM, PRAM). Съем дампа памяти устройства, содержащего микропрограммный код. Возможность взаимодействия с микросхемами различных типов корпусов (PLCC, DIP, SIP/PDIP/CDIP, LCC, TSOP, ZIP, SOIC/SO/SQP, QFP/TQFP/LQFP, SSOP)				+	+	+				+	+	+
30	Средства анализа бинарного кода (дизассемблеры, декомпиляторы, деобфускаторы, распаковщики, средства восстановления формата данных)	Получение восстановленного кода программы путем выполнения преобразования машинного кода в код на языке assembler (дизассемблирования), в код на языке высокого уровня (декомпилирования). Преодоление механизмов защиты от исследования бинарного кода (восстановление программы из упакованного исполняемого файла, преобразование запутанного (обфусцированного) кода программы к виду, удобному для его дальнейшего анализа. Возможность выявления программных ошибок в результате анализа восстановленного кода программы. Возможность интеграции с отладчиком и анализатором трасс				+	+	+				+	+	+
31	Средства динамического анализа	Получение трассы выполнения в рамках разработанных тестовых сценариев. Возможность разметки трассы на нити и процессы, определение в трассе фактического размещения				+	+	+				+	+	+

[illegible]

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
32	Средства композиционного анализа	Ведение перечня программных компонент, входящих в состав исследуемого программного обеспечения в машиночитаемом формате. Возможность импорта и экспорта перечня программных компонент, входящих в состав программного обеспечения средств защиты информации. Возможность периодической актуализации в автоматическом режиме сведения о наличии уязвимостей в программных компонентах, входящих в состав программного обеспечения. Формирование отчетов о выявленных уязвимостях. Средства композиционного анализа должны обеспечивать реализацию положений Методики выявления уязвимостей и недеklarированных возможностей в программном обеспечении, утвержденной ФСТЭК России 16 мая 2026 г.				+	+	+				+	+	+

* Виды работ и услуг установлены пунктом 3 Положения о лицензировании деятельности по разработке и производству, утвержденного постановлением Правительства Российской Федерации от 3 марта 2012 г. № 171 (СЗКИ – средства защиты конфиденциальной информации).

ПРИМЕЧАНИЕ:

1. Работы и услуги, указанные в подпунктах а1, а2, а3, б1, б2, б3 (столбцах 4, 5, 6, 10, 11, 12), проводятся и оказываются при разработке и производстве средств защиты конфиденциальной информации, предназначенных для выявления и предотвращения утечки защищаемой информации по техническим каналам.

2. Работы и услуги, указанные в подпунктах а4, а5, а6, б4, б5, б6 (столбцах 7, 8, 9, 13, 14, 15), проводятся и оказываются при разработке и производстве средств защиты конфиденциальной информации, предназначенных для исключения или существенного затруднения несанкционированного доступа к защищаемой информации и предотвращения специальных программно-технических воздействий на информацию (носители информации), вызывающих нарушение конфиденциальности, целостности или доступности защищаемой информации.

3. При выборе контрольно-измерительного и испытательного оборудования, средств контроля эффективности защиты (защищенности) информации, используемых (планируемых к использованию) при осуществлении деятельности по разработке и производству средств защиты конфиденциальной информации, приоритет следует отдавать оборудованию (средствам), произведенному (разработанным) на территории Российской Федерации.