"Перечень контрольно-измерительного и испытательного оборудования, средств контроля защищенности, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79" (утв. ФСТЭК России 19.04.2017)

Утверждаю
Директор ФСТЭК России
В.Селин
19 апреля 2017 г.

№ п/п	Наименование оборудования	Технические и (или) функциональные характеристики	Вид работ и (или) услуг[1)]
1.	Генераторы шумовых сигналов	Вид шумового сигнала: - «белый шум» (с нормальным распределением плотности вероятности мгновенных значений); - хаотическая импульсная последовательность. Диапазон частот 175...5600 Гц	а.3, а.4, г.2, г.3, е.1, е.2, е.3
2.	Низкочастотные генераторы сигналов	Диапазон частот 175...5600 Гц. Выходное напряжение не менее 5 В	а.3, а.4, г.2, г.3, е.1, е.2, е.3
3.	Усилители мощности	Диапазон частот 175...5600 Гц. Выходная мощность не менее 10 Вт	а.3, а.4, г.2, г.3, е.1, е.2, е.3
4.	Акустические излучатели	Диапазон воспроизводимых частот 175 ... 5600 Гц. Уровень звукового давления на расстоянии 1 м от излучателя в свободном поле не менее 95 дБ. Неравномерность АЧХ не более 6 дБ	а.3, а.4, г.2, г.3, е.1, е.2, е.3
5.	Измерители шума и вибраций (шумомеры)	Диапазон частот 175...5600 Гц. Пределы измерения уровней сигналов 25...120 дБ. Класс точности не ниже 2-го	а.3, а.4, г.2, г.3, е.1, е.2, е.3
6.	Селективные микровольтметры	Диапазон частот 175...5600 Гц. Погрешность измерения не более 15%	а.1, г.1, г.2, г.3, е.1, е.2, е.3
7.	Измерительные приемники (анализаторы спектра)	Диапазон измеряемых параметров 9 кГц...1000 МГц. Погрешность измерения не более 2 дБ	а.1, г.1, г.2, г.3, е.1, е.2, е.3
8.	Селективные нановольтметры	Диапазон частот 175...5600 Гц. Погрешность измерения не более 15%	а.1, а.2, а.3, а.4, г.2, г.3, е.1, е.2, е.3
9.	Измерительные микрофоны	Диапазон частот 175...5600 Гц. Чувствительность не хуже 10 мВ/Па. Неравномерность АЧХ 1 дБ	а.3, а.4, г.2, г.3, е.1, е.2, е.3
10.	Измерительные антенны	Диапазон измеряемых частот: по магнитной составляющей 9 кГц ... 30 МГц; по электрической составляющей 9 кГц ... 1000 МГц. Погрешность измерения не более 2 дБ	а.1, а.2, г.1, е.1, е.2, е.3
11.	Вибродатчики (акселерометры)	Диапазон частот 175...5600 Гц. Чувствительность не хуже 1 мВ/мс-1. Неравномерность АЧХ не более 10%	а.3, а.4, г.2, г.3
12.	Измерительные пробники	Диапазон измеряемых параметров 9 кГц...300 МГц	а.1, а.2, г.1, е.1, е.2, е.3
13.	Полосовые октавные фильтры со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц	Диапазон частот 175...5600 Гц. Номинальное ослабление в полосе пропускания фильтра 0 дБ. Класс точности 1-й или 2-й АЧХ в соответствии с ГОСТ 17168-82	а.3, а.4, г.2, г.3, е.1, е.2, е.3
14.	Осциллографы	Диапазон измеряемых параметров 0...5 МГц	а.1, а.2, г.1, е.1, е.2, е.3
15[2)].	Оптические тестеры (измерители мощности)	Длина волны калибровки, нм 850, 1310, 1550. Диапазон измерений оптической мощности дБ, от 3 до минус 10 - минус 73. Разрешающая способность, дБ -0,1...0,001	а.1, а.2, г.1, г.2, е.1, е.2, е.3
16[3)].	Рефлектометры (микрорефлектометры)	Длина волны калибровки, нм 850, 1310, 1550. Диапазон измерений оптической мощности дБ, от 3 до минус 26 - минус 65. Разрешение по затуханию, дБ - 0,001	а.1, а.2, г.1, г.2, е.1, е.2, е.3

17[4].	Программные средства автоматизированного проектирования	Автоматизация проектирования объектов информатизации	д
18.	Программные средства формирования и контроля полномочий доступа в информационных (автоматизированных) системах	Формирование и контроль полномочий доступа для автономных автоматизированных рабочих мест и сетей, серверов, работающих с тонкими клиентами, и компьютеров, функционирующих в распределенных сетях. Должны иметь сертификаты соответствия ФСТЭК России	б, г.1, д.1
19.	Средства поиска остаточной информации на машинных носителях информации	Поиск остаточной информации на машинных носителях информации. Должны иметь сертификаты соответствия ФСТЭК России	б, г.1
20.	Средства контроля подключения устройств	Сбор информации о подключении съемных машинных носителей информации и других устройств к средствам вычислительной техники. Должны иметь сертификаты соответствия ФСТЭК России	б, г.1
21.	Программные средства контроля целостности	Расчет уникальных значений контрольных сумм. Документирование результатов расчета контрольных сумм. Должны иметь сертификаты соответствия ФСТЭК России	б, г.1, д.1
22.	Средства (системы) контроля (анализа) защищенности информационных систем	Автоматизированная инвентаризация ресурсов информационных систем (сбор информации об узлах информационных систем и об используемом в них программном обеспечении), выявление уязвимостей (кода, конфигурации и архитектуры) в них, анализ и управление выявленными уязвимостями с учетом угроз. Должны иметь сертификаты соответствия ФСТЭК России	б, в, г.1, д.1
23.	Замкнутые среды предварительного выполнения программ («песочницы»)	Среды безопасного выполнения программ в целях анализа их влияния на безопасность информации. Должны иметь формуляры, оформленные разработчиками (производителями) данных сред. В случае невозможности оформления формуляров разработчиками (производителями) данных сред (свободнораспространяемое программное обеспечение) формуляры оформляются лицензиатами (соискателями лицензии)	в
24.	Средства управления информацией об угрозах безопасности информации	Автоматизированный сбор и анализ информации, поступающей из различных источников, об угрозах безопасности информации. Должны иметь формуляры, оформленные разработчиками (производителями) данных средств. В случае невозможности оформления формуляров разработчиками (производителями) данных средств (свободнораспространяемое программное обеспечение) формуляры оформляются лицензиатами (соискателями лицензии)	в
25.	Средства управления событиями безопасности информации	Автоматизированный сбор, анализ и корреляция данных о событиях безопасности информации, регистрируемых компонентами информационных систем, идентификация по заданным индикаторам типовых инцидентов информационной безопасности и их локализация. Должны иметь сертификаты соответствия ФСТЭК России	в
26.	Средства управления инцидентами информационной безопасности	Автоматизированная регистрация информации об инцидентах информационной безопасности информационных систем, предоставление рекомендаций по реагированию на них, формирование и модификация шаблонов инцидентов информационной безопасности, в том числе рекомендаций по реагированию на них. Должны иметь формуляры, оформленные разработчиками (производителями) данных средств. В случае невозможности оформления формуляров разработчиками (производителями) данных средств (свободнораспространяемое программное обеспечение) формуляры оформляются лицензиатами (соискателями лицензии)	в
27.	Средства защиты каналов передачи данных	Должны обеспечивать конфиденциальность и целостность данных, передаваемых по каналам связи между информационной системой, используемой для управления информационной безопасностью, и информационными системами, в отношении которых осуществляется мониторинг. Должны иметь сертификаты соответствия ФСБ России	в
28.	Системы защиты информации информационных систем, используемых для мониторинга информационной безопасности	Системы защиты информации информационных систем, используемых для оказания услуг по мониторингу информационной безопасности информационных систем, должны соответствовать Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. № 17, применительно к первому классу защищенности государственных информационных систем	в

техническая защита информации, аттестация, сертификация

[1] Перечень работ и услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 03.02.2012 № 79:

а) контроль защищенности конфиденциальной информации от утечки по техническим каналам в:

1 - средствах и системах информатизации;

2 - технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается;

3 - помещениях со средствами (системами), подлежащими защите;

4 - помещениях, предназначенных для ведения конфиденциальных переговоров (далее - защищаемые помещения);

б) контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
в) мониторинг информационной безопасности средств и систем информатизации;
г) аттестационные испытания и аттестация на соответствие требованиям по защите информации:
1 - средств и систем информатизации;
2 - помещений со средствами (системами), подлежащими защите;
3 - защищаемых помещений;
д) проектирование в защищенном исполнении:
1 - средств и систем информатизации;
2 - помещений со средствами (системами), подлежащими защите;
3 - защищаемых помещений;
е) установка, монтаж, испытания, ремонт средств защиты информации:
1 - технических средств защиты информации;
2 - защищенных технических средств обработки информации;
3 - технических средств контроля эффективности мер защиты информации;
4 - программных (программно-технических) средств защиты информации;
5 - защищенных программных (программно-технических) средств обработки информации;
6 - программных (программно-технических) средств контроля защищенности информации).
[2], [3] Средства необходимы при проведении работ (оказании услуг) при применении волоконно-оптических систем передачи информации.
[4] Средства необходимы при проектировании комплексов помещений (зданий, сооружений), а также сложных распределенных объектов защиты.

From:
http://sps-ib.ru/ - **Справочно-правовая система по информационной безопасности**

Permanent link:
http://sps-ib.ru/npa:fstek_19.04.2017

Last update: **2017/05/25 11:45**