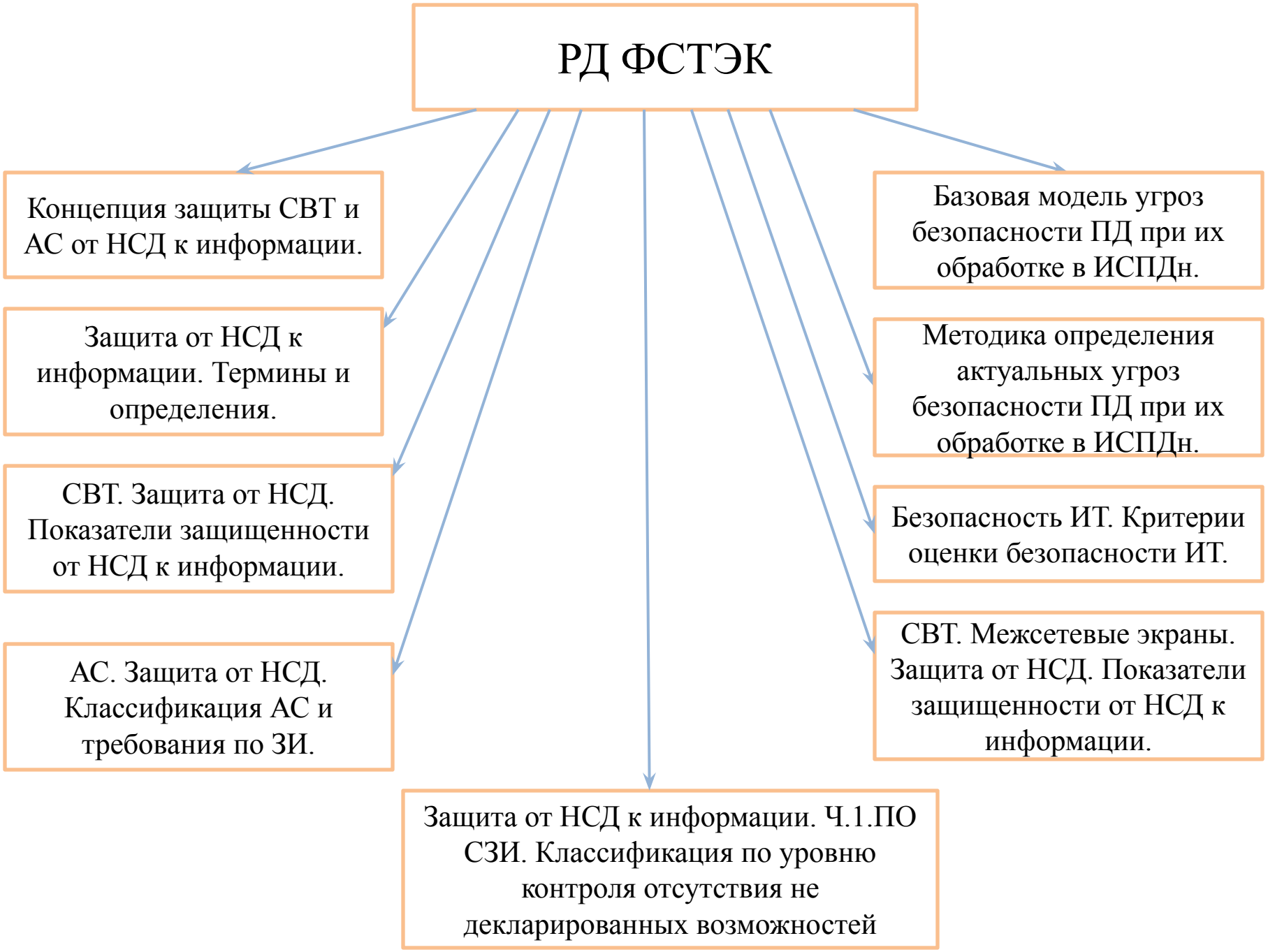
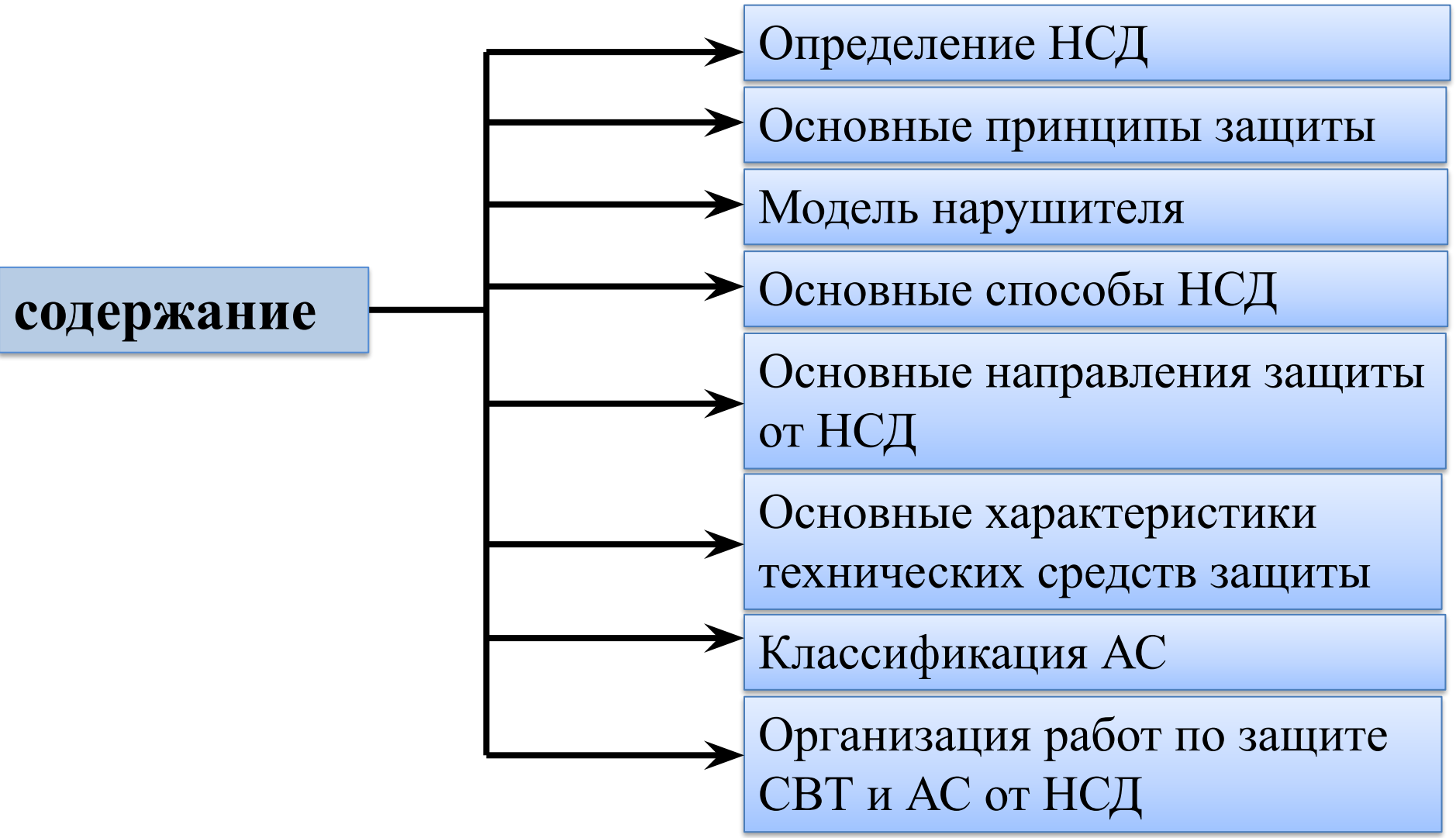
Системы ЗИ от несанкционированного доступа


РД ФСТЭК
Концепция защиты СВТ и АС от НСД к информации.
Защита от НСД к информации. Термины и определения.
СВТ. Защита от НСД. Показатели защищенности от НСД к информации.
АС. Защита от НСД. Классификация АС и требования по ЗИ.
Защита от НСД к информации. Ч.1.ПО СЗИ. Классификация по уровню контроля отсутствия не декларированных возможностей
Базовая модель угроз безопасности ПД при их обработке в ИСПДн.
Методика определения актуальных угроз безопасности ПД при их обработке в ИСПДн.
Безопасность ИТ. Критерии оценки безопасности ИТ.
СВТ. Межсетевые экраны. Защита от НСД. Показатели защищенности от НСД к информации.

Руководящий документ «Концепция защиты средств ВТ и АС от НСД»



Определение НСД

НСД определяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС.

Под *штатными средствами* понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС.

Направления в проблеме ЗИ от НСД

Средства вычислительной техники (СВТ)

совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.
СВТ разрабатываются и поставляются лишь как элементы, из которых в дальнейшем строятся функционально ориентированные АС, и поэтому, не решая прикладных задач, СВТ не содержат пользовательской информации

Автоматизированные системы (АС)

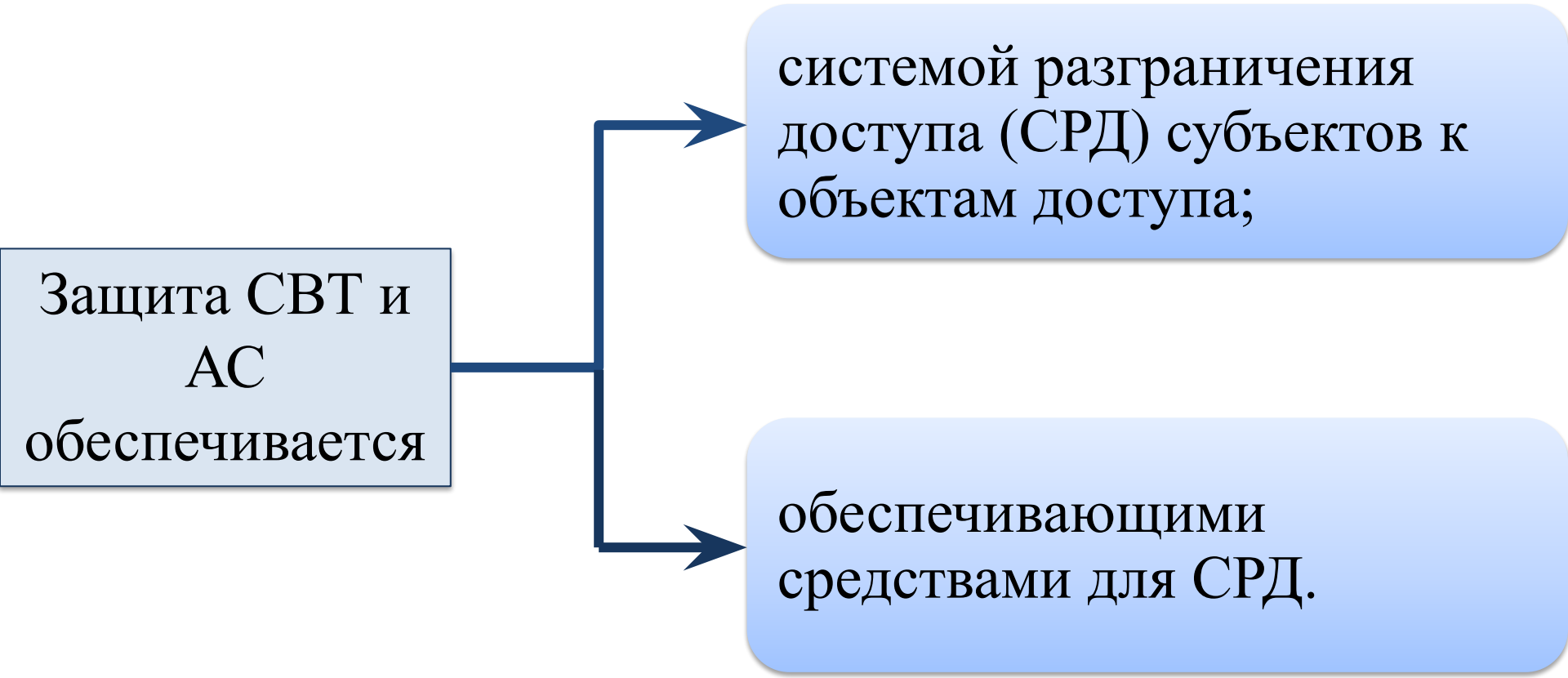
система обработки данных. Помимо пользовательской информации, при создании АС появляются такие отсутствующие при разработке СВТ характеристики АС, как полномочия пользователей, модель нарушителя, технология обработки информации


Основные принципы защиты
Защита СВТ и АС основывается на положениях и требованиях существующих законов, нормативных документов по защите от НСД;
Защита СВТ и АС обеспечивается комплексом программно-технических средств
Защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования
средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации)
Неотъемлемой частью работ по защите является оценка эффективности средств защиты
Защита АС должна предусматривать контроль эффективности средств защиты от НСД

Основные способы НСД

- непосредственное обращение к объектам доступа;
- создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
- модификация средств защиты, позволяющая осуществить НСД;
- внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД.

Основные направления защиты от НСД



Основные функции СРД


Функции обеспечивающих средств для СРД
идентификация и аутентификация субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;
регистрация действий субъекта
исключения и включения новых субъектов и объектов доступа, изменение полномочий субъектов;
реакция на попытки НСД, например, сигнализацию, блокировку, восстановление после НСД;
тестирование;
очистка оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;

Основные характеристики технических средств защиты

- степень полноты охвата ПРД реализованной СРД и ее качество;
- состав и качество обеспечивающих средств для СРД;
- гарантии правильности функционирования СРД и обеспечивающих ее средств.

Модель нарушителя

Нарушитель-субъект, имеющий доступ к работе со штатными средствами АС и СВТ

Классификация по уровню предоставляемых возможностей

1) Запуск программ из фиксированного набора (самый низкий уровень);

2) Запуск собственной программы с новыми функциями по обработке информации;

3) Управление функционированием АС,т.е воздействие на базовое ПО, состав и конфигурирование оборудования;

4) Весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт ТС АС, вплоть до включения в состав СВТ собственных ТС с новыми функциями по обработке информации.

РД ФСТЭК «Средства вычислительной техники. Защита от несанкционированного доступа»

ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации»

Классы защищенности

Верифицированная защита

Осуществляется верификация соответствия объектного кода тексту системы защиты на языке высокого уровня

Требования к классам защищенности СВТ

Наименование	6	5	4	3	2	1
Дискреционный контроль доступа	+	+	+	=	+	+
Мандатный контроль доступа	-	-	+	=	=	=
Очистка памяти	-	+	+	+	=	=
Изоляция модулей	-	-	+	=	+	=
Маркировка документов	-	-	+	=	=	=
Защита ввода/вывода на отчуждаемый носитель	-	-	+	=	=	=
Сопоставление пользователя с устройством	-	-	+	=	=	=
Идентификация и аутентификация	+	=	+	=	=	=
Гарантии проектирования	-	+	+	+	+	+
Регистрация	-	+	+	+	=	=
Взаимодействие пользователя с КСЗ	-	-	-	+	=	=
Надежное восстановление	-	-	-	+	=	=

Требования к классам защищенности СВТ

Наименование	6	5	4	3	2	1
Целостность КСЗ	-	+	+	+	=	=
Контроль модификации	-	-	-	-	+	=
Контроль дистрибуции	-	-	-	-	+	=
Гарантии архитектуры	-	-	-	-	-	+
Тестирование	+	+	+	+	+	=
Руководство пользователя	+	+	+	+	+	=
Руководство по КСЗ	+	+	=	+	+	=
Тестовая документация	+	+	+	+	+	=
Конструкторская документация	+	+	+	+	+	+


Требования к разграничению доступа
Дискреционный принцип контроля
Очистка оперативной и внешней памяти
Мандатный принцип контроля
Изоляция программных модулей процессов
Установка меток на устройства ввода-вывода и каналы связи

Дискреционный принцип защиты

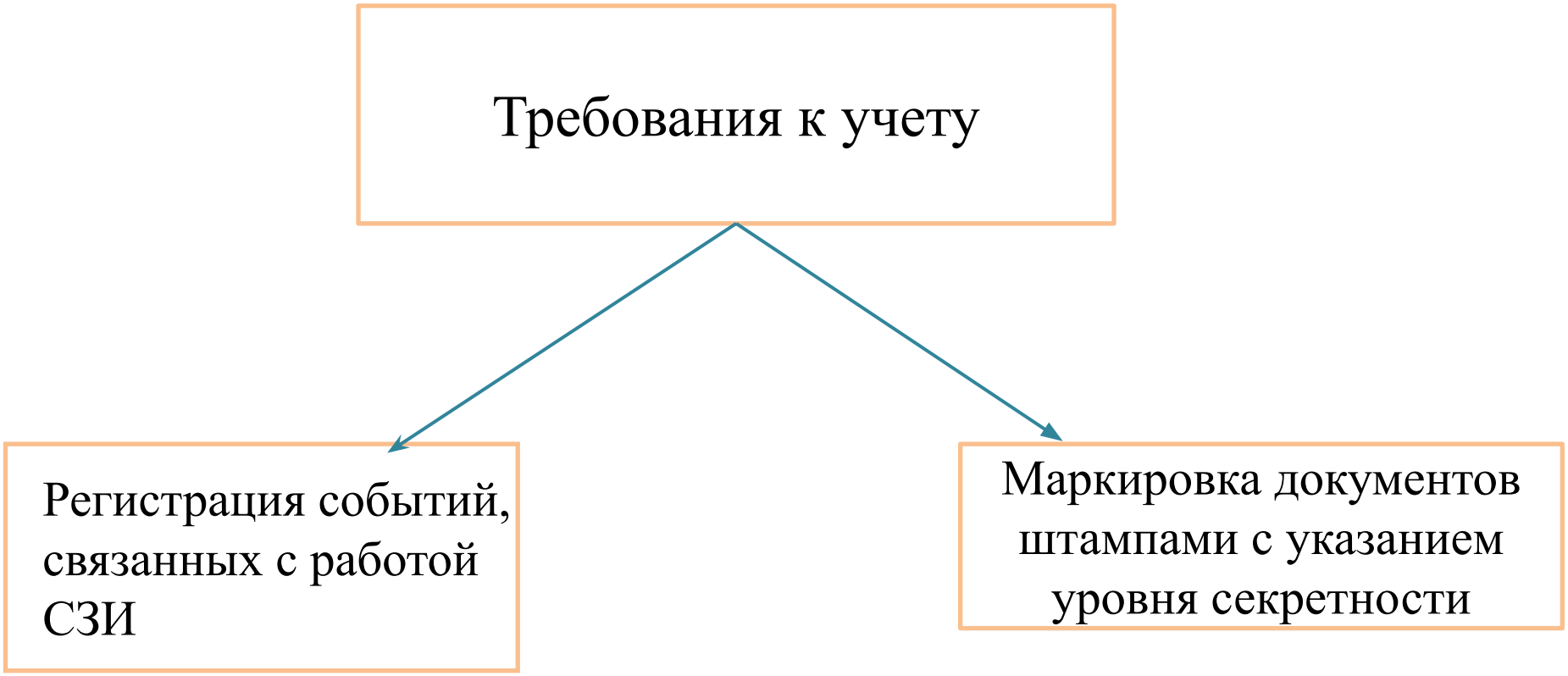
Для каждой пары пользователь – объект (ресурс) задается явное перечисление допустимых типов доступа, то есть задается матрица доступа

	Ресурс 1	Ресурс 2	Ресурс 3
Петя	R	RW	-
Рашид	R	-	RW
Костя	RW	R	R

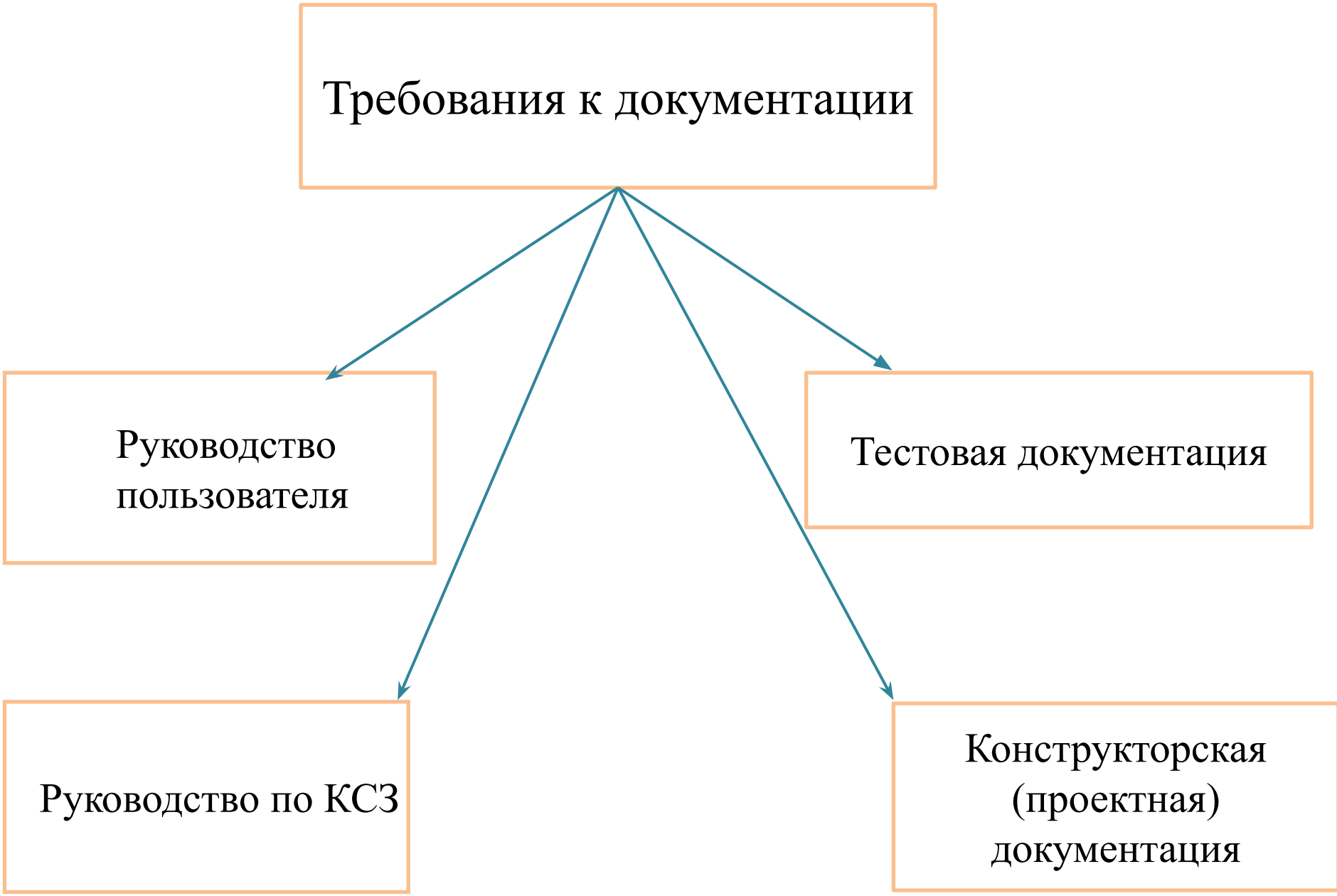
Мандатная защита

Каждому пользователю (субъекту) и объекту (файлу, каталогу, принтеру) должны сопоставляться классификационные метки, характеризующие категории секретности.

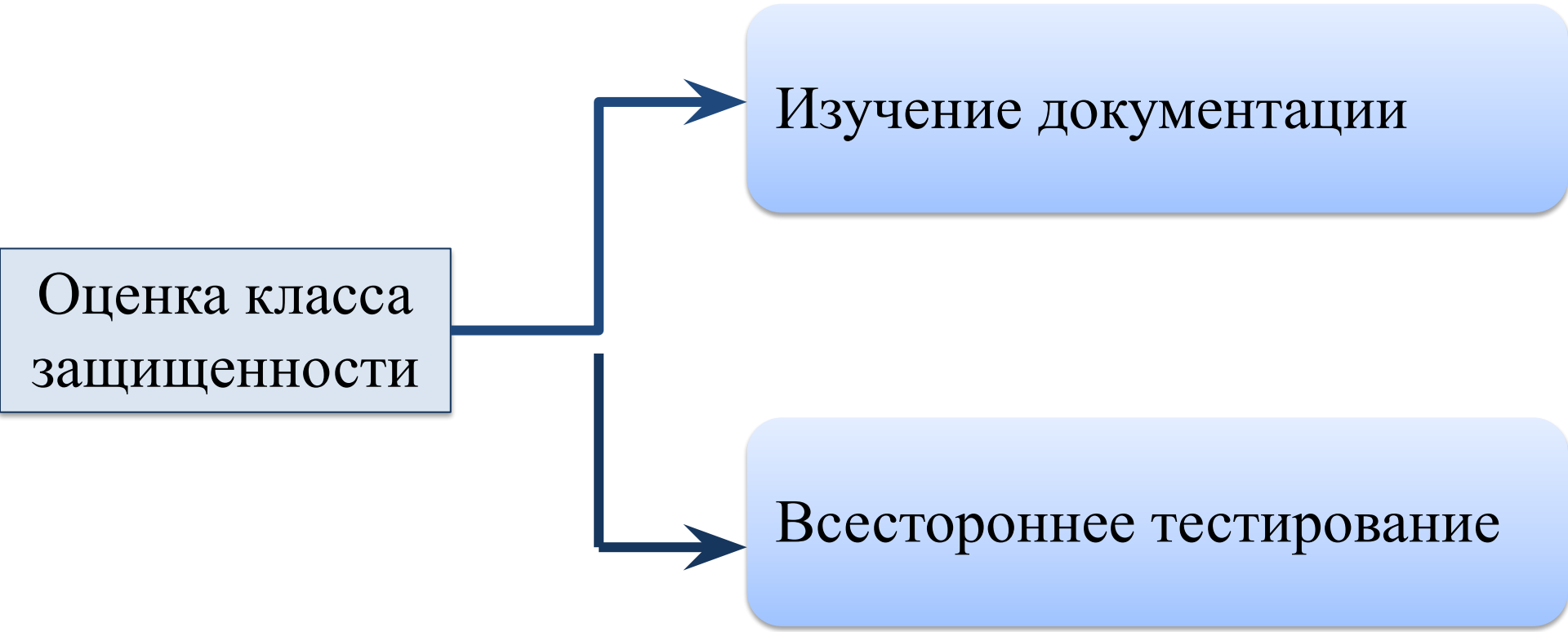
Субъект может получить доступ к объектам, чей уровень секретности не выше его собственного и не может записать информацию в объекты с меньшим уровнем секретности.


Требования к учету
Регистрация событий, связанных с работой СЗИ
Маркировка документов штампами с указанием уровня секретности


Требования к гарантиям
Гарантии проектирования
Надежное восстановление
Целостность КСЗ
Контроль модификации
Контроль дистрибуции
Гарантии архитектуры
Взаимодействие пользователя с КСЗ
Тестирование

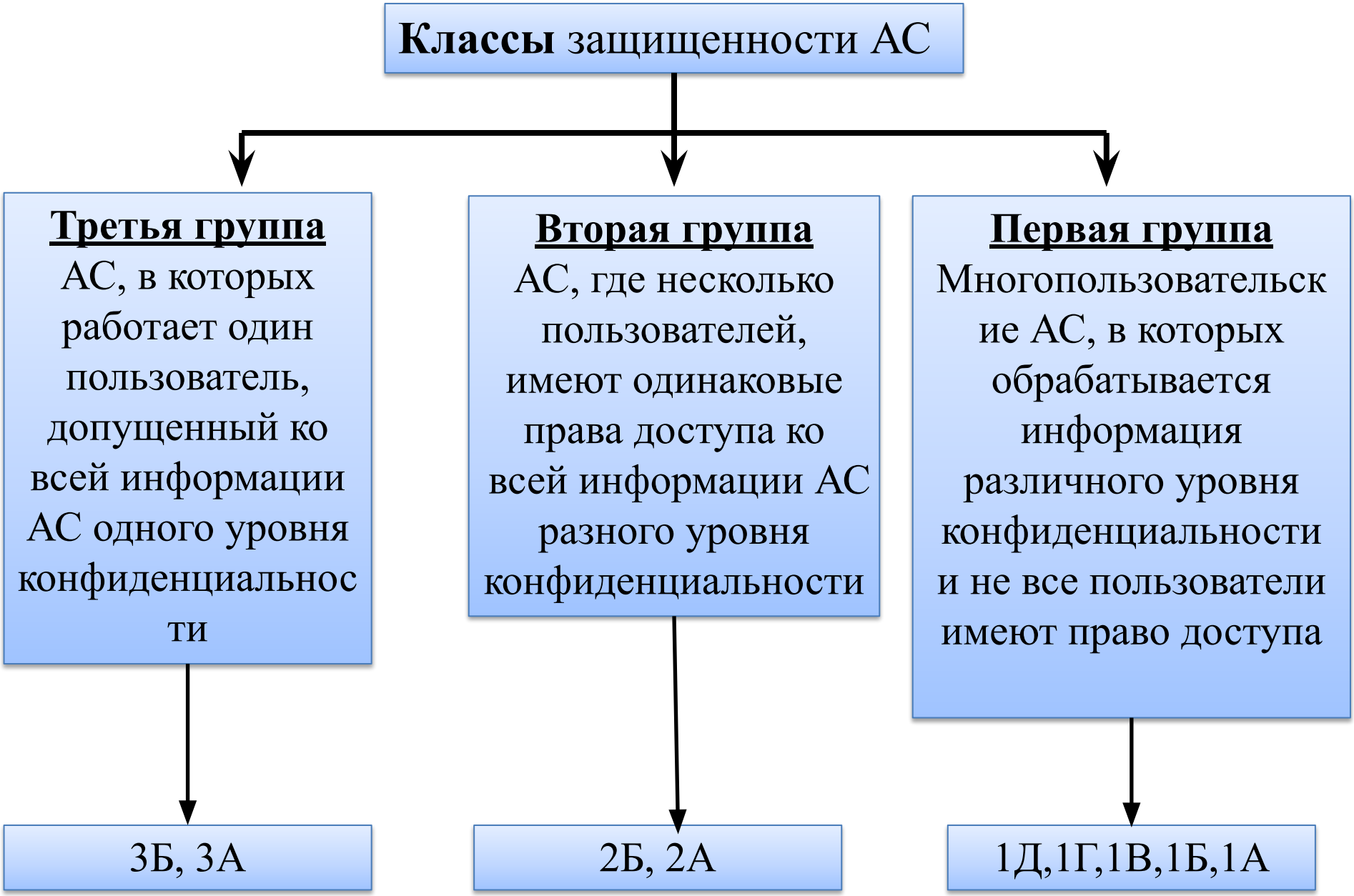

Требования к документации
Руководство пользователя
Тестовая документация
Руководство по КСЗ
Конструкторская (проектная) документация

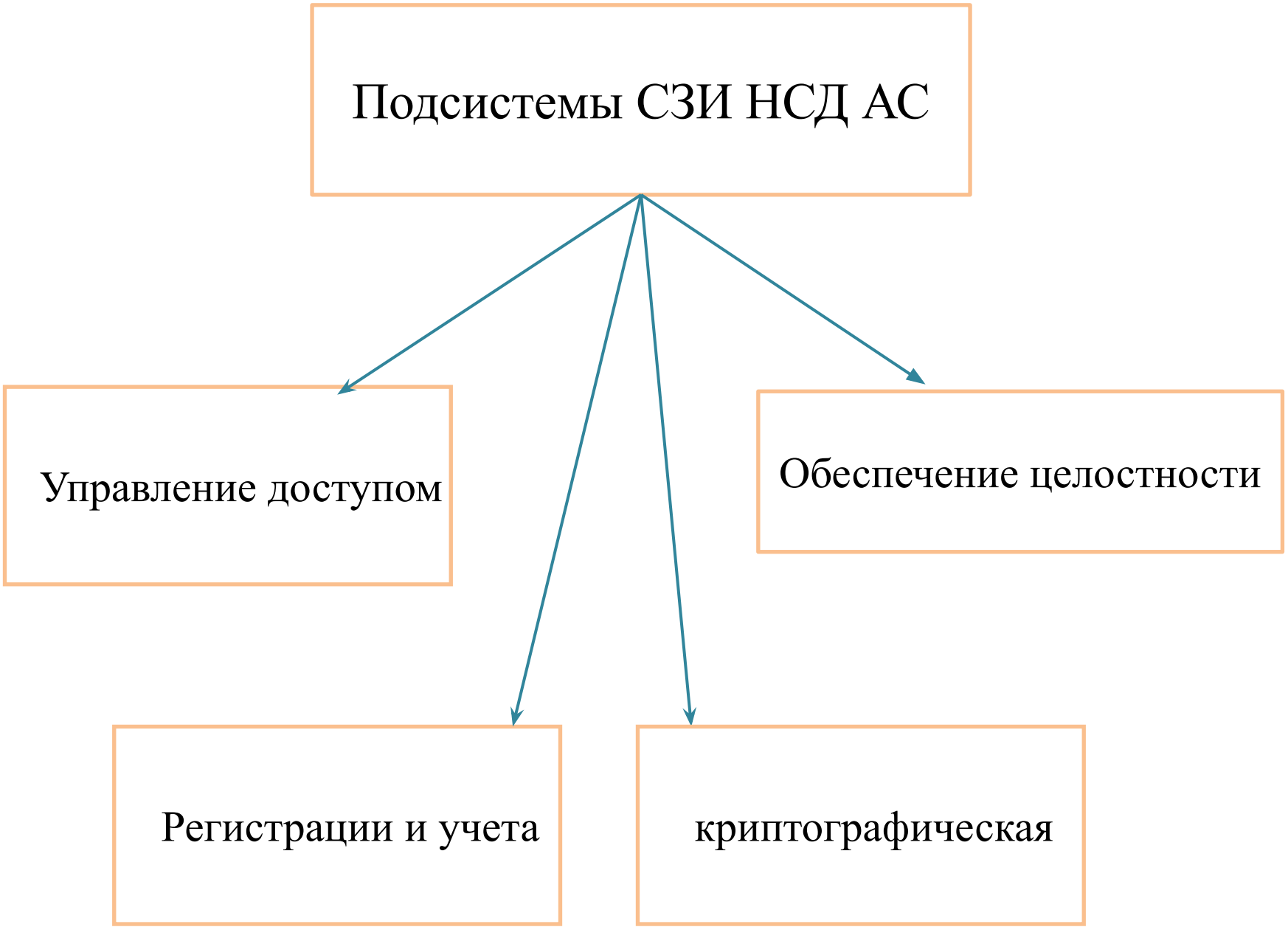
Основные направления защиты от НСД




Техническое заключение
описание комплекса средств защиты
оценка класса защищенности СВТ
наличие и соответствие дополнительных требований
аргументация оценки (объяснение соответствия КСЗ требованиям, посредством чего обеспечивается выполнение каждого требования);
описание испытаний, которым подвергалось СВТ (с указанием состава технических и программных средств);
объяснение, почему СВТ не может быть сертифицировано по более высокому классу защищенности
Другие положения и выводы, необходимые по мнению экспертов

РД ФСТЭК «Автоматизированные системы. Защита от несанкционированного доступа»


Классы защищенности АС
Третья группа
АС, в которых работает один пользователь, допущенный ко всей информации АС одного уровня конфиденциальности
Вторая группа
АС, где несколько пользователей, имеют одинаковые права доступа ко всей информации АС разного уровня конфиденциальности
Первая группа
Многопользовательские АС, в которых обрабатывается информация различного уровня конфиденциальности и не все пользователи имеют право доступа
3Б, 3А
2Б, 2А
1Д,1Г,1В,1Б,1А


Подсистемы СЗИ НСД АС
Управление доступом
Обеспечение целостности
Регистрации и учета
криптографическая

Требования по защищенности к АС

Подсистемы и требования		Классы								
		3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
1		2	3	4	5	6	7	8	9	10
1. Подсистема управления доступом										
1.1.	Идентификация, проверка подлинности и контроль доступа субъектов:									
	• в систему;	+	=	+	=	3Б	2Б	=	+	+
	• к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ;	-	-	-	+	-	+	+	+	+
	• к программам;	-	-	-	+	-	+	=	=	+
	• к томам, каталогам, файлам, записям, полям записей	-	-	-	+	-	+	=	=	+
1.2.	Управление потоками информации	-	-	-	+	-	-	2А	=	=

Требования по защищенности к АС

Подсистемы и требования		Классы								
		3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
1		2	3	4	5	6	7	8	9	10
2. Подсистема регистрации и учета										
2.1.	Регистрация и учет:									
	• входа/выхода субъектов доступа в/из системы (узла сети);	+	+	3А	+	2А	+	=	=	=
	• выдачи печатных (графических) выходных документов;	-	+	-	+	-	2А	+	+	=
	• запуска/завершения программ и процессов (заданий, задач);	-	-	-	+	-	2А	=	+	+
	• доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи;	-	-	-	+	-	2А	+	=	=
	• доступа программ к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;	-	-	-	+	-	2А	+	=	=
	• изменения полномочий субъектов доступа;	-	-	-	-	-	-	+	+	=
	• создаваемых защищаемых объектов доступа	-	-	-	+	-	-	+	+	=
2.2.	Учет носителей информации.	+	+	3Б	+	+	=	+	+	=
2.3.	Очистка (обнуление, обезличивание) освобождаемых областей ОЗУ ЭВМ и внешних накопителей	-	+	-	3А	-	+	+	=	=
2.4.	Сигнализация попыток нарушения защиты	-	-	-	-	-	-	+	+	=
3. Криптографическая подсистема										

Требования по защищенности к АС

Подсистемы и требования		Классы								
		3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
1		2	3	4	5	6	7	8	9	10
3. Криптографическая подсистема										
3.1.	Шифрование конфиденциальной информации	-	-	-	+	-	-	-	2 А	=
3.2.	Шифрование информации, принадлежащей различным субъектам доступа на разных ключах	-	-	-	-	-	-	-	-	+
3.3.	Использование сертифицированных криптографических средств.	-	-	-	+	-	-	-	2 А	=

Требования по защищенности к АС

Подсистемы и требования		Классы								
		3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
1		2	3	4	5	6	7	8	9	10
4. Подсистема обеспечения целостности										
4.1.	Обеспечение целостности программных средств и обрабатываемой информации.	+	=	3Б	=	+	=	=	+	+
4.2.	Физическая охрана СВТ и носителей информации.	+	+	3Б	3А	3Б	=	+	=	=
4.3.	Наличие администратора (службы) защиты информации в АС.	-	-	-	+	-	-	+	=	=
4.4.	Периодическое тестирование СЗИ НСД.	+	=	3Б	=	3Б	=	+	=	=
4.5.	Наличие средств восстановления СЗИ НСД.	+	=	3Б	=	3Б	=	=	+	=
4.6.	Использование сертифицированных средств защиты.	-	+	-	3А	-	-	3А	=	=

РД. АС. Защита от НСД. Классификация АС и требования по ЗИ

Категория информации	Класс АС	Класс СВТ
ОВ	3А,2А,1А	2
СС	3А,2А,1Б	3
С	3А,2Б,1В	4
Служебная тайна	3Б,2Б,1Г	
Персональные данные	3Б,2Б,1Д	

РД. ПО СЗИ. Классификация по уровню контроля отсутствия НДВ

Набор требований:

- контроль состава и содержание документации;
- контроль исходного состояния ПО;
- статический анализ текстов программ;
- динамический анализ текстов программ;
- отчетность.

Перечень требований к уровню контроля

N	Наименование требования	Уровень контроля			
		4	3	2	1
	Требования к документации				
1	Контроль состава и содержания документации				
1.1.	Спецификация (ГОСТ 19.202-78)	+	=	=	=
1.2.	Описание программы (ГОСТ 19.402-78)	+	=	=	=
1.3.	Описание применения (ГОСТ 19.502-78)	+	=	=	=
1.4.	Пояснительная записка (ГОСТ 19.404-79)	-	+	=	=
1.5.	Тексты программ, входящих в состав ПО (ГОСТ 19.401-78)	+	=	=	=
	Требования к содержанию испытаний				
2.	Контроль исходного состояния ПО	+	=	=	=
3.	Статический анализ исходных текстов программ				
3.1.	Контроль полноты и отсутствия избыточности исходных текстов	+	+	+	=
3.2.	Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду	+	=	=	+
3.3.	Контроль связей функциональных объектов по управлению	-	+	=	=
3.4.	Контроль связей функциональных объектов по информации	-	+	=	=
3.5.	Контроль информационных объектов	-	+	=	=
3.6.	Контроль наличия заданных конструкций в исходных текстах	-	-	+	+
3.7.	Формирование перечня маршрутов выполнения функциональных объектов	-	+	+	=
3.8.	Анализ критических маршрутов выполнения функциональных объектов	-	-	+	=
3.9.	Анализ алгоритма работы функциональных объектов на основе блок-схем, диаграмм и т. п., построенных по исходным текстам контролируемого ПО	-	-	+	=
4.	Динамический анализ исходных текстов программ				
4.1.	Контроль выполнения функциональных объектов	-	+	+	=
4.2.	Сопоставление фактических маршрутов выполнения функциональных объектов и маршрутов, построенных в процессе проведения статического анализа	-	+	+	=
5.	Отчетность	+	+	+	+

Обозначения:
"-" - нет требований к данному уровню;
"+" - новые или дополнительные требования;
"=" - требования совпадают с требованиями предыдущего уровня.

РД. ПО СЗИ. Классификация по уровню контроля отсутствия НДВ

Категория информации	Требуемый класс уровня контроля НДВ
ОВ	1
СС	2
С	3
конфиденциальная	4

РД «Критерии оценки безопасности информационных технологий.

Гриф информации	Класс защищенности изделий ИТ	Оценочный уровень доверия
ОВ	1	ОУД 6
СС	2	ОУД 5
С	3	ОУД 4
Конфиденц.	4	ОУД 1

Соответствие категории информации классам защищенности

Категория информации	Класс АС	Класс СВТ	Класс уровня контроля НДВ	Класс защищенности изделий ИТ	Оценочный уровень доверия
1. Наиболее секретная информация (особой важности)	3А, 2А,1А	Не менее 2	1	1	6
2. Менее секретная (СС)	3А, 2А, 1Б	3	2	2	5
3. Секретная информация	3А, 2Б, 1Б	4	3	3	4
4.Конфиденциальная информация	3Б, 2Б, 1Г (служебная тайна) 3Б, 2Б, 1Д (персональные данные)	-	4	4	1

Защищенные операционные системы

ОС	N серти-фика	Срок действия	Класс Защиты
Windows XP SP3	844/3	12.14	ОУД 1(усил)
Windows Server 2003 EE R2	1017/7	09.14	ОУД1(усил)
Windows Vista	1516	11.13	ОУД1(усил)
Windows Server 2008 R2	2181	10.14	ОУД1, 1Г(АС),2(ИСПД)
Windows 7	2180, 2417	08.14	5(СВТ), 1Г(АС).2(ИСПД)
Windows Server 2012	2949-2952	09.16	5(СВТ)
Windows 8	2960	09.16	5(СВТ)

Защищенные операционные системы

ОС	N серти-фика	Срок действия	Класс Защиты
Циркон10С	1945	11.15	3(СВТ), 2(НДВ)
Циркон 10Кр2, 26К	2443,2778	12.15	5(СВТ), 4(НДВ)
Solaris10	1582	03.14	5(СВТ), 1Г(АС)
ОС РВ QNX	906	05.16	3(СВТ), 2(НДВ),1Б (АС)
Янукс3.0	1651	07.14	ОУД3+,4(НДВ),К1(ИСПД)
ALT Linux 6	2317	04.14	4(СВТ),3(НДВ)
МСВСфера Desktop, Server	2079,2080	04.16	ОУД2, 4(НДВ),1Г(АС), К1(ИСПД)

Состав сертифицированной ФСТЭК версии

Состав	Пакет поставки		
	базовый	Базовый контроль	полный
Верифицированный установочный комплект ПО	+	+	+
Бессрочный абонент на сертифиц. online – обновления	+	+	+
Копия сертификата ФСТЭК, формуляр с голограммой	+	+	+
Формуляр и лицензии на ПО Check контроля сертифиц. версии ПО (по кол-ву раб.мест с сертифиц ПО)	+	+	+
Media-Kit (CD) А) ПО контроля сертифицированной версии ПО; Б) рук-во по настройке, контролю, получению обновлений сертифиц. ПО; В) ПО для eToken Г) инф. материалы	+	+	+
USB eToken Pro с цифровым сертификатом для получения обновлений	+	+	+

Цены на пакеты сертификации (на 03.2013)

	Базовый	Полный	Лицензия на ПО контроля
XP Prof	1350	2870	550
Win 7 Проф	1620	3170	648
Win 7 Корп	2105	3569	756
Win 7 Макс	2105	-	1263
Office 2007 Standart	3100	-	1240
Office 2010 Prof Plus	3825	-	1340
Server 2003 St	6525	8045	2895
Server 2003 Ent	20735	22255	8294
Server 2008 R2 St	7500	-	2800
Server 2008 R2 Ent	24640	-	8960
SQL Serv 2008 St	8470	-	2680
SQL Serv 2005 Ent	69700	-	24614

Цены на пакеты сертификации (на 12.2009)

	Базовый	Б.контроль	Полный	Лицензия на ПО контроля
XP Prof	800	1050	2662	550
Vista Business	900	-	-	600
Vista Ultimate	1134	-	-	756
Office 2003	1840	-	-	1205
Office 2007 Standart	1860	-	-	1240
Office 2007 Prof	2010	-	-	1340
Server 2003 St	3630	-	5492	2895
Server 2003 Ent	12441	-	14303	8294
Server 2008 St	4200	-	-	2800
Server 2008 Ent	13440	-	-	8960
SQL Serv 2005 St	4020	-	-	2680
SQL Serv 2005 Ent	37271	-	-	24614

Цены на сертифицированные USB ключи

Ключ	Цена, $
eToken Pro/32Кб для сертифицированных обновлений	38,42
eToken Pro/32Кб для усиленной аутентификации пользователей	49

Разновидности Secure Pack Rus

1.0		АК1/АК2	Усилен аутентиф(1), контр целостн
2.0 (исп 3)	X64	АК2	+усил аудит, центр контроль
2.0 (исп 2)	X86	АК2	
2.0 (исп 1)	X86	АК3	+аудит печати+контр внешн носит

Цены на Secure Pack Rus 2.0

Secure Pack Rus	Цена	Цена, руб
	1 исп	2 исп
For Windows XP	4000	3150
For Windows Server (без КриптоПроTLS)	10000	9300
For Windows Server (с КриптоПро TLS)	33000	20000
Дистрибутив		660

Офисные пакеты и базы данных

	N серти-фика	Срок действия	Класс защиты
Oracle 10g	1583	03.14	5(СВТ),1Г (АС),2(ИСПД)
Линтер 6.0 (Бастион)	2601	03.15	2(СВТ),2(НДВ)
MS BizTalk Server 2009	2438	09.14	1Г(АС), 2(ИСПД)
MS Exchange Server 2007 SP1	1814|1	04.14	5(СВТ), 2(ИСПД),1Г
MS Office 2007	1923	10.15	ОУД1(усил), 1Г,
MS Office 2010	2590	03.15	ТУ

Прикладные пакеты

	N серти-фика	Срок действия	Класс защиты
Docs Vision 4.5	2118	06.16	5(СВТ),1Г (АС),2(ИСПД)
MS Dynamics AX,NAV,CRM	2090-2092	05.13	1Г(АС), 2(ИСПД)
ИВК БюрократЪ	2152	08.13	2(НДВ)
1С Предприятие 8.2	2137	07.13	5(СВТ),4(НДВ), 1Г(АС),К1(ИСПД)

Порядок разработки защищенных СВТ

(Временное Положение
по организации разработки, изготовления и эксплуатации программных и технических СЗИ от НСД в АС и СВТ)

1. Разработка защищенных СВТ осуществляется по госзаказу в соответствии с ТЗ, согласованным с ФСТЭК России (в случае встроенных криптосредств с Главным шифрорганом страны).

2. При разработке защищенных программных средств на базе импортных программных прототипов необходимо снятие защиты от копирования и вскрытия механизма работы прототипа, а также проведение анализа защитных средств прототипа на предмет их соответствия требованиям ТЗ с целью использования задействованных средств защиты, их дополнения и модификации.

3. Предприятия, осуществляющие разработку защищенных СВТ обязаны разрабатывать тестовые программные средства, позволяющие проконтролировать достигнутый уровень защищенности.

Присвоение грифа секретности

- Гриф секретности действующих сменных ключей и соответствующих ключевых документов при защите информации от НСД с помощью СКЗИ, должен соответствовать максимальному грифу секретности информации, шифруемой с использованием этих ключей
- СКЗИ без введенных криптографических констант и действующих сменных ключей имеют гриф секретности, соответствующий грифу описания криптосхемы.
- СКЗИ с загруженными криптографическими константами имеет гриф секретности, соответствующий грифу криптографических констант.
- Гриф секретности СКЗИ с загруженными криптографическими константами и введенными ключами определяется максимальным грифом содержащихся в СКЗИ ключей и криптографических констант