Выполнение сертифицированными механизмами защиты информации из состава **КСЗИ «Панцирь-К»** требований Приказа ФСТЭК России от 11 февраля 2013 г. **№ 17**, Приказа ФСТЭК России от 18 февраля 2013 г. **№ 21**

	№ 17	**№ 21**
Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)		
ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора **в части доступа в информационную систему**	+ **Усиления - 1б, 2б, 3, 4, 5, 6**	+
ИАФ.2 Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	+	+
ИАФ.3 Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+
ИАФ.4 Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+ **Усиление - 1а, 1б, 1в, 1г**	+
ИАФ.5 Защита обратной связи при вводе аутентификационной информации	+	+
ИАФ.7 Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа	+	Мера отсутствует
Управление доступом субъектов доступа к объектам доступа (УПД)		
УПД.1 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+
УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа **в части реализации иных методов**	+ **Усиления - 1, 2, 3, 4**	+
УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	+
УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+
УПД.6 Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+ **Усиление - 1**	+
Ограничение программной среды (ОПС)		
ОПС.1 Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения	+ **Усиления - 1**	+
Защита машинных носителей информации (ЗНИ)		
ЗНИ.8 Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)	+ **Усиления -3, 5г**	+

Регистрация событий безопасности (РСБ)		
РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+
РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+
РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения	+ **Усиления - 1,**	+
РСБ.7 Защита информации о событиях безопасности	+	+
РСБ.8 Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе	+ **Усиление - 1**	Мера отсутствует
Обеспечение целостности информационной системы и информации (ОЦЛ)		
ОЦЛ.1 Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	+ **Усиление - 1**	+
Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)		
ЗИС.15 Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации	+	+

Меры защиты и обеспечения безопасности информации, не указанные в приведенном списке, либо являются необязательными для выполнения, либо должны реализовываться организационными мерами, либо соответствующими средствами защиты прикладного уровня.