Выполнение сертифицированными механизмами защиты информации из состава **КСЗИ «Панцирь+»** и **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	+ **Усиление - 2**	+
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.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+ **Усиление - 1**	+
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**	+
УПД.10 Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	+	+
УПД.12 Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки	+	+

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, 2, 3, 5, 6**	+
ОПС.4 Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов	+	+
Защита машинных носителей информации (ЗНИ)		
ЗНИ.2 Управление доступом к машинным носителям информации	+	+
ЗНИ.5 Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	+ **Усиление - 1**	+
ЗНИ.6 Контроль ввода (вывода) информации на машинные носители информации	+	+
ЗНИ.7 Контроль подключения машинных носителей информации	+ **Усиления - 1, 2**	+
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	+ **Усиление - 2**	+
РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+ **Усиление - 2**	+
РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения	+ **Усиления - 1, 2, 3**	+
РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти **в части защиты от переполнения объема памяти**	+	+
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**	+
ОЦЛ.3 Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	+	+
ОЦЛ.6 Ограничение прав пользователей по вводу информации в информационную систему	+	+
Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)		
ЗИС.1 Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и	+	+

иных функций информационной системы		
ЗИС.5 Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	+	+
ЗИС.8 Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи	+	+
ЗИС.9 Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации	+	+
ЗИС.15 Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации	+	+
ЗИС.18 Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения	+	+
ЗИС.21 Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы	+	Мера отсутствует
ЗИС.23 Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями	+	Мера отсутствует
ЗИС.24 Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения	+	Мера отсутствует
Выявление инцидентов и реагирование на них (ИНЦ)		
ИНЦ.3 Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами **в части информирования о возникновении инцидентов**	Мера отсутствует	+
Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)		
УКФ.4 Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных	Мера отсутствует	+
Контроль (анализ) защищенности персональных данных (АНЗ)		
АНЗ.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе	**Усиление - 1**	Мера отсутствует

Желтым выделены меры защиты и обеспечения безопасности информации, которые реализует КСЗИ «Панцирь+» и КСЗИ «Панцирь-К».

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.