# ВЫПОЛНЕНИЕ МЕР 31-ГО ПРИКАЗА ФСТЭК ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ПУТЕМ ПРИМЕНЕНИЯ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА «СЕКРЕТ ОСОБОГО НАЗНАЧЕНИЯ»

**ОКБ САПР**

**2021**

## 1 Общие положения

В настоящем документе рассматривается выполнение мер 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения программно-аппаратного комплекса «Секрет Особого Назначения» (далее – ПАК «Секрет Особого Назначения», «Секрет Особого Назначения», СН либо комплекс).

ПАК «Секрет Особого Назначения» представляет собой это защищенный служебный носитель информации, предназначенный для таких задач, когда данные, конфиденциальность которых должна контролироваться, должны храниться на служебном носителе и переноситься сотрудником в рамках его должностных обязанностей на различные компьютеры.

ПАК «Секрет Особого Назначения» включает:

– специальный носитель «Секрет Особого Назначения» (СН);
– программное обеспечение (ПО) рабочей станции (РС) – консоль администратора и консоль пользователя.

Консоль администратора необходима для администрирования СН (установки списка разрешенных РС, длины пароля, возможного числа попыток аутентификации пользователя и т.д.). Консоль пользователя предназначена для выполнения авторизации пользователя и получения доступа к закрытому разделу диска СН.

ПАК «Секрет Особого Назначения» предназначен как для корпоративного, так и для личного использования.

Основные особенности:

– диск ПАК «Секрет Особого Назначения» состоит из двух разделов: открытого и закрытого. ПО РС размещается на открытом диске СН, на котором и исполняется (без установки на жесткий диск РС). Закрытый раздел диска предназначен для хранения и переноса данных пользователя;

– доступ к закрытому разделу диска СН предоставляется только после успешного завершения контрольных процедур;

– ведется аппаратный журнал работы СН, содержащийся на закрытом разделе диска СН. Журнал работы СН недоступен для пользователя и позволяет увидеть все случаи подключения устройства к каким-либо компьютерам, даже те, что закончились неуспешно;

– предусмотрена возможность задания списка РС, на которых разрешено использование СН. На неразрешенных компьютерах – будь то в корпоративной сети или вне ее, «Секрет Особого Назначения» не примонтируется.

## 2 Выполнение базового набора мер, определенных 31-ым приказом ФСТЭК России по защите информации в автоматизированной системе управления, путем применения ПАК «Секрет Особого Назначения»

В таблице № 1 представлено описание выполнения базового набора мер 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения ПАК «Секрет Особого Назначения» (ТУ 4012-033-11443195-2012).

Выражение «все» в ячейках столбца «Классы защищенности автоматизированной системы управления» означает, что рассматриваемая мера должна быть реализована в информационной системе с любым классом защищенности.

**Таблица 1 – Выполнение базового набора мер по защите информации 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения ПАК «Секрет Особого Назначения»**

| № | Усл. обозн. и номер меры | Меры защиты информации в автоматизированных системах безопасности | Классы защищенности автоматизированной системы управления | «Секрет Особого Назначения» | Ссылки на документацию |
|---|---|---|---|---|---|
| | | **Идентификация и аутентификация (ИАФ)** | | | |
| 1 | ИАФ.0 | Разработка политики идентификации и аутентификации | + все | В комплексе разработана политика идентификации и аутентификации. | |
| 2 | ИАФ.1 | Идентификация и аутентификация пользователей и инициируемых ими процессов | + все | Идентификация администратора производится по логину, а аутентификация – по паролю.<br>Идентификация пользователя производится по логину пользователя а аутентификация – по коду авторизации (КА). | 1. п.п. 3.1 документа «Секрет Особого Назначения. Руководство администратора»;<br>2. п.п. 3.2 документа «Секрет Особого Назначения. Руководство пользователя». |
| 3 | ИАФ.2 | Идентификация и аутентификация устройств | + все | Идентификация РС в ПАК «Секрет Особого Назначения» выполняется по следующим параметрам: серийный номер «Аккорд-АМДЗ», серийный номер материнской платы компьютера, серийный номер дистрибутива ОС, идентификатор домена Active Directory, имя компьютера в домене. | 1. п.п. 3.2.2 документа «Секрет Особого Назначения. Руководство администратора». |
| 4 | ИАФ.4 | Управление средствами аутентификации | + все | Создание и смена пароля администратора, установка длины КА пользователя, установка числа ошибок авторизации пользователя выполняется администратором СН в консоли администратора.<br>Создание и смена КА пользователя выполняется пользователем СН в консоли пользователя. | 1. п.п. 3.1, 3.2, 3.5, 3.6, 3.10 документа «Секрет Особого Назначения. Руководство администратора»;<br>2. п.п. 3.1, 3.2, 3.4, 3.5 документа «Секрет Особого Назначения. Руководство пользователя». |
| 5 | ИАФ.7 | Защита аутентификационной информации при передаче | + все | При вводе пароль администратора и КА пользователя отображаются символами. | |
| | | **Управление доступом (УПД)** | | | |
| 6 | УПД.0 | Разработка политики управления доступом | + все | В комплексе разработана политика управления доступом. | |
| 7 | УПД.1 | Управление учетными записями пользователей | + все | Комплекс обеспечивает управление учетными записями пользователей СН.<br>Возможные операции с пользователями: создание, редактирование настроек доступа учетной записи, аннулирование регистрации пользователя. | 1. п.п. 3 документа «Секрет Особого Назначения. Руководство администратора»;<br>2. п.п. 3 документа «Секрет Особого Назначения. Руководство пользователя». |
| 8 | УПД.2 | Реализация политик | + | В комплексе реализован | 1. п.п. 2.2, 3.1 документа |

| № | Усл. обозн. и номер меры | Меры защиты информации в автоматизированных системах безопасности | Классы защищенности автоматизированной системы управления | «Секрет Особого Назначения» | Ссылки на документацию |
|---|---|---|---|---|---|
| | | управления доступом | все | ролевой метод разграничения доступа. | «Секрет Особого Назначения. Руководство администратора»;<br>2. п.п. 3.1 документа «Секрет Особого Назначения. Руководство пользователя». |
| 9 | УПД.4 | Разделение полномочий (ролей) пользователей | +<br>все | В случае личного использования СН пользователь является также администратором устройства. В этом случае пользователю доступны функции управления устройством (посредством консоли администратора).<br>Администратору доступны функции управления устройством (создание списка разрешенных РС, установка типа доступа к СН, установка типа заполнения журнала, числа ошибок авторизации пользователя и т.д.). Пользователю данные функции не доступны.<br>Пользователю после успешного завершения авторизации доступен закрытый раздел диска СН, к которому администратор получить доступ не может. | 1. п.п. 3, 6 документа «Секрет Особого Назначения. Руководство администратора»;<br>2. п.п. 3 документа «Секрет Особого Назначения. Руководство пользователя». |
| 10 | УПД.5 | Назначение минимально необходимых прав и привилегий | +<br>все | | |
| 11 | УПД.6 | Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему | +<br>все | Администратор СН может установить для пользователя необходимое количество неуспешных попыток авторизации.<br>Это число может варьироваться в пределах от 1 до 255 (по умолчанию установлено значение 3). | 1. п.п. 3.2.4 документа «Секрет Особого Назначения. Руководство администратора». |
| 12 | УПД.9 | Ограничение числа параллельных сеансов доступа | +<br>в 1 классе защищенности автоматизированной системы управления | Для каждой учетной записи возможен только один сеанс доступа.<br>При попытке запустить консоль пользователя при работающей консоли администратора на экране появляется следующее сообщение | |
| 13 | УПД.11 | Управление действиями пользователей до идентификации и аутентификации | +<br>все | До проведения идентификации и аутентификации пользователю запрещены любые действия кроме ввода идентификационной и аутентификационной информации. | 1. п.п. 4 документа «Секрет Особого Назначения. Руководство пользователя». |
| 14 | УПД.14 | Контроль доступа из внешних информационных (автоматизированных) систем | +<br>все | | 1. п.п. 3.2.2 документа «Секрет Особого Назначения. Руководство администратора». |
| | | **Защита машинных** | | | |

| № | Усл. обозн. и номер меры | Меры защиты информации в автоматизированных системах безопасности | Классы защищенности автоматизированной системы управления | «Секрет Особого Назначения» | Ссылки на документацию |
|---|---|---|---|---|---|
| | | **носителей информации (ЗНИ)** | | | |
| 15 | ЗНИ.0 | Разработка политики защиты машинных носителей информации | + все | В ПАК «Секрет Особого Назначения» реализована политика защиты машинных носителей информации. | |
| 16 | ЗНИ.2 | Управление физическим доступом к машинным носителям информации | + все | ПАК «Секрет Особого Назначения» позволяет управлять доступом к СН: ограничить работу СН на РС (настройка «Доступ с ограничением по доменам и рабочим станциям») – создать список разрешенных РС, временно снять все ограничения на доступ к СН на РС, редактировать список разрешенных РС, настроить политику использования КА пользователя. | 1. п.п. 3.2, 3.3 документа «Секрет Особого Назначения. Руководство администратора». |
| 17 | ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации | + все | При выборе настройки «Доступ с ограничением по доменам и рабочим станциям» возможно ограничить использование СН на РС (создать список РС, на которых разрешено использование СН), тем самым, можно контролировать перенос информации на СН между РС корпоративной сети или вне ее. | 1. п.п. 3.3 документа «Секрет Особого Назначения. Руководство администратора». |
| 18 | ЗНИ.6 | Контроль ввода (вывода) информации на машинные носители информации | + В 1 классе защищенности автоматизированной системы управления | | |
| 19 | ЗНИ.7 | Контроль подключения машинных носителей информации | + все | | |
| 20 | ЗНИ.8 | Уничтожение (стирание) информации на машинных носителях информации | + все | Комплекс обеспечивает полное удаление информации пользователя с закрытого раздела диска СН, а также аннулирование регистрации администратора, сброс всех настроек СН, удаление журнала событий, аннулирование регистрации пользователя СН (функция «Общий сброс СН»).<br>При выборе данной функции выполняется возврат устройства к заводским настройкам. | 1. п.п. 3.6, 3.8 документа «Секрет Особого Назначения. Руководство администратора». |
| | | **Аудит безопасности (АУД)** | | | |
| 21 | АУД.0 | Разработка политики аудита безопасности | + все | В ПАК «Секрет Особого Назначения» реализована политика аудита безопасности. | |
| 22 | АУД.2 | Анализ уязвимостей и их устранение | + все | Устранение уязвимостей комплекса выполняется путем установки обновлений программного обеспечения средств защиты информации.<br>Обновление прошивки СН выполняется в сервисном центре Разработчика ПО. | 1. п. 6 документа «Секрет Особого Назначения. Формуляр». |

| № | Усл. обозн. и номер меры | Меры защиты информации в автоматизированных системах безопасности | Классы защищенности автоматизированной системы управления | «Секрет Особого Назначения» | Ссылки на документацию |
|---|---|---|---|---|---|
| 23 | АУД.3 | Генерирование временных меток и (или) синхронизация системного времени | +<br>все | В ПАК «Секрет Особого Назначения» имеется возможность установки внутреннего времени (в том случае, если СН снабжен внутренними часами).<br>Если СН снабжен внутренними часами, события регистрируются в журнале в соответствии с установленным на них временем. | 1. п.п. 3.9 документа «Секрет Особого Назначения. Руководство администратора». |
| 24 | АУД.4 | Регистрация событий безопасности | +<br>все | В ПАК «Секрет Особого Назначения» ведется аппаратный журнал регистрации событий СН, который содержит информацию о событиях, зафиксированных в процессе работы с ПАК «Секрет Особого Назначения» на конкретной РС. | 1. п.п. 3.4 документа «Секрет Особого Назначения. Руководство администратора». |
| 25 | АУД.6 | Защита информации о событиях безопасности | +<br>все | Доступ к журналу событий ПАК «Секрет Особого Назначения» имеет только администратор устройства. Пользователь имеет доступ к журналу событий только при личном использовании СН.<br>Для доступа к журналу событий предоставляется только после успешного выполнения процедуры авторизации. | |
| 26 | АУД.7 | Мониторинг безопасности | +<br>все | Комплекс обеспечивает просмотр администратору зарегистрированных в журнале событий безопасности, экспорт журнала в текстовый файл и очистку журнала. | 1. п.п. 3.4, 7 документа «Секрет Особого Назначения. Руководство администратора». |
| 27 | АУД.8 | Реагирование на сбои при регистрации событий безопасности | +<br>все | В журнале событий фиксируются ошибки, которые могут возникнуть при работе СН.<br>Запись в журнале с сообщением об ошибке содержит номер ошибки, позволяющий разработчикам продукта определить её причину при обращении в техническую поддержку изготовителя. | 1. п.п. 3.2.3, 3.4 документа «Секрет Особого Назначения. Руководство администратора». |
| 28 | АУД.9 | Анализ действий пользователей | +<br>в 1 классе защищенности автоматизированной системы управления | Администратору доступна функция фильтрации событий по следующим параметрам:<br>– период времени. Можно задать начало и/или конец интересующего периода времени, используя строки «С:» и «По:»;<br>– тип события. Доступен просмотр событий типов «Сообщение», «Ошибка», «Предупреждение», а также одновременный просмотр событий всех типов (значение параметра «Все»); | 1. п.п. 3.4 документа «Секрет Особого Назначения. Руководство администратора». |

| № | Усл. обозн. и номер меры | Меры защиты информации в автоматизированных системах безопасности | Классы защищенности автоматизированной системы управления | «Секрет Особого Назначения» | Ссылки на документацию |
|---|---|---|---|---|---|
| | | | | – исполнитель. Доступен просмотр событий, связанных с работой ПО, администратора или пользователя, а также одновременный просмотр событий для всех исполнителей (значение параметра «Все»);<br>– имя РС;<br>– домен;<br>– описание события. | |
| | | **Обеспечение целостности (ОЦЛ)** | | | |
| 29 | ОЦЛ.0 | Разработка политики обеспечения целостности | +<br>все | В комплексе реализована политика обеспечения целостности | |
| 30 | ОЦЛ.1 | Контроль целостности программного обеспечения | +<br>все | Целостность встраиваемого ПО обеспечивается технологически в процессе производства ПАК «Секрет Особого Назначения»: контроль пользователя и консоль администратора из состава ПО ПАК «Секрет Особого Назначения» располагаются на открытом разделе диска CH, защищенном от записи (в режиме «только чтение»). | 1. п.п. 2.2 документа «Секрет Особого Назначения. Руководство администратора». |
| 31 | ОЦЛ.3 | Ограничение по вводу информации в информационную (автоматизированную) систему | +<br>в 1 классе защищенности автоматизированной системы управления | Ограничение прав пользователей по вводу информации в информационную систему обеспечивается за счет выполнения мер УПД.4 и УПД.5. | 1. п.п. 3 документа «Секрет Особого Назначения. Руководство администратора»;<br>2. п.п. 3 документа «Секрет Особого Назначения. Руководство пользователя». |
| 32 | ОЦЛ.5 | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях | +<br>начиная со 2 класса защищенности автоматизированной системы управления | При ошибочных действиях пользователя возникают соответствующие предупреждения. | 1. п.п. 3.2 документа «Секрет Особого Назначения. Руководство администратора»;<br>2. п. 3 документа «Секрет Особого Назначения. Руководство пользователя». |
| | | **Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)** | | | |
| 33 | ЗИС.0 | Разработка политики защиты информационной (автоматизированной) системы и ее компонентов | +<br>все | Комплекс обеспечивает защиту информационной (автоматизированной) системы и ее компонентов в части изоляции процессов в выделенной области памяти, защиты неизменяемых данных | |
| 34 | ЗИС.1 | Разделение функций по управлению (администрированию) информационной (автоматизированной) | +<br>все | Имеется возможность разделения функций по управлению информационной системой: поддерживаются роли администратора и пользователя | 1. п.п. 2.2, 3.1 документа «Секрет Особого Назначения. Руководство администратора»; |

| № | Усл. обозн. и номер меры | Меры защиты информации в автоматизированных системах безопасности | Классы защищенности автоматизированной системы управления | «Секрет Особого Назначения» | Ссылки на документацию |
|---|---|---|---|---|---|
| | | системой с иными функциями | | устройства. | 2. п.п. 3.1 документа «Секрет Особого Назначения. Руководство пользователя». |
| 35 | ЗИС.13 | Защита неизменяемых данных | + во 2 классе защищенности автоматизированной системы управления | Технологически в процессе производства ПАК «Секрет Особого Назначения» обеспечивается целостность встраиваемого ПО. | |
| 36 | ЗИС.20 | Обеспечение доверенных канала, маршрута | + все | В ПАК «Секрет Особого Назначения» имеется возможность создания списка разрешенных РС.<br>Администратор и пользователь выполняют функции безопасности на рабочей станции из числа разрешенных. | 1. п.п. 3.2.2, 3.3 документа «Секрет Особого Назначения. Руководство администратора». |
| 37 | ЗИС.33 | Исключение доступа через общие ресурсы | + в 1 классе защищенности автоматизированной системы управления | В случае необходимости возврата устройства к заводским настройкам имеется функция общего сброса СН. | 1. п.п. 3.8 документа «Секрет Особого Назначения. Руководство администратора». |
| | | **Реагирование на компьютерные инциденты (ИНЦ)** | | | |
| 38 | ИНЦ.0 | Разработка политики реагирования на компьютерные инциденты | + все | В ПАК «Секрет Особого Назначения» реализованы механизмы регистрации и предупреждения (сигнализации) о событиях, относящихся к возможным нарушениям безопасности.<br>Выполняется регистрация следующих событий:<br>– начало сеанса работы СН с рабочей станции;<br>– установка внутренних часов СН;<br>– установка описания рабочей станции;<br>– регистрация администратора;<br>– смена пароля администратора;<br>– установка политик КА;<br>– установка политик доступа к рабочей станции;<br>– установка политик записи журнала СН;<br>– очистка журнала СН;<br>– полный сброс СН;<br>– получение доступа к журналу событий;<br>– обновление внутреннего ПО СН;<br>– регистрация пользователя;<br>– аннулирование регистрации | |
| 39 | ИНЦ.1 | Выявление компьютерных инцидентов | + все | | |
| 40 | ИНЦ.2 | Информирование о компьютерных инцидентах | + все | | |

| № | Усл. обозн. и номер меры | Меры защиты информации в автоматизированных системах безопасности | Классы защищенности автоматизированной системы управления | «Секрет Особого Назначения» | Ссылки на документацию |
|---|---|---|---|---|---|
| | | | | пользователя;<br>– смена КА;<br>– блокирование СН;<br>– разблокирование СН;<br>– авторизация пользователя. | |
| | | **Управление обновлениями программного обеспечения (ОПО)** | | | |
| 41 | ОПО.0 | Разработка политики управления обновлениями программного обеспечения | +<br>все | Комплекс обеспечивает возможность установки обновлений внутреннего программного обеспечения СН (прошивки). | |
| 42 | ОПО.4 | Установка обновлений программного обеспечения | +<br>все | | 1. п. 6 документа «Секрет Особого Назначения. Формуляр». |

## 3 Выполнение дополнительных (не включенных в базовый набор) мер, определенных 31-ым приказом ФСТЭК России по защите информации в автоматизированной системе управления, путем применения ПАК «Секрет Особого Назначения»

В таблице № 2 представлено описание выполнения дополнительных (не включенных в базовый набор) мер 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения ПАК «Секрет Особого Назначения» (ТУ 4012-033-11443195-2012).

**Таблица 2 - Выполнение дополнительных (не включенных в базовый набор) мер по защите информации 31-го приказа ФСТЭК по защите информации в автоматизированной системе управления путем применения ПАК «Секрет Особого Назначения»**

| № | Усл. обозн. и номер меры | Меры защиты информации в автоматизированных системах безопасности | Классы защищенности автоматизированной системы управления | «Секрет Особого Назначения» | Ссылки на документацию |
|---|---|---|---|---|---|
| | | **Защита машинных носителей информации (ЗНИ)** | | | |
| 1 | ЗНИ.3 | Контроль перемещения машинных носителей | | В ПАК «Секрет Особого Назначения» имеется возможность установки политики доступа к СН с ограничением по доменам и рабочим станциям. | 1. п.п. 3.2 документа «Секрет Особого Назначения. Руководство администратора». |
| 2 | ЗНИ.4 | Исключение возможности несанкционированного чтения информации на машинных носителях | | На РС из списка разрешенных доступ к закрытому разделу диска СН, на котором хранятся пользовательские данные, предоставляется только после | 1. п.п. 3.2.2, 3.3 документа «Секрет Особого Назначения. Руководство администратора». |

| № | Усл. обозн. и номер меры | Меры защиты информации в автоматизированных системах безопасности | Классы защищенности автоматизированной системы управления | «Секрет Особого Назначения» | Ссылки на документацию |
|---|---|---|---|---|---|
| | | информации | | успешного завершения контрольных процедур.<br>На неразрешенных компьютерах «Секрет Особого Назначения» не примонтируется, соответственно, несанкционированное ознакомление с содержанием персональных данных исключается. | |
| | | **Обеспечение целостности (ОЦЛ)** | | | |
| 3 | ОЦЛ.2 | Контроль целостности информации | | Посредством применения СН исключаются раскрытие, несанкционированная модификация данных пользователя на РС, не входящих в список разрешенных. | 1. п.п. 3.3 документа «Секрет Особого Назначения. Руководство администратора». |
| | | **Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)** | | | |
| 4 | ЗИС.10 | Использование программного обеспечения, функционирующего в средах различных операционных систем | | ПАК «Секрет Особого Назначения» может использоваться в ОС семейства Windows, Linux. | 1. п.п. 1.1 документа «Секрет Особого Назначения. Руководство администратора». |
| 5 | ЗИС.12 | Изоляция процессов (выполнение программ) в выделенной области памяти | | Диск ПАК «Секрет Особого Назначения» разделен на открытый (в режиме «только чтение») и закрытый разделы.<br>На открытом разделе диска СН, защищенном от записи, располагается и исполняется ПО ПАК «Секрет Особого Назначения».<br>Закрытый раздел диска СН предназначен для хранения и переноса данных. Доступ к закрытому разделу диска СН получает только пользователь СН после прохождения процедур авторизации. | 1. п.п. 2.2 документа «Секрет Особого Назначения. Руководство администратора». |
| 6 | ЗИС.14 | Использование неперезаписываемых машинных носителей информации | | ПО РС располагается на открытом разделе диска СН, доступном только для чтения.<br>ПАК «Секрет Особого Назначения» обеспечивает исполнение ПО РС непосредственно со СН. Установки на РС не требуется. | 1. п.п. 1.1 документа «Секрет Особого Назначения. Руководство администратора». |
| 7 | ЗИС.17 | Защита информации от утечек | | ПАК «Секрет Особого Назначения» является средством, способным оказать содействие в блокировании в ИС скрытых каналов передачи информации. | |

| № | Усл. обозн. и номер меры | Меры защиты информации в автоматизированных системах безопасности | Классы защищенности автоматизированной системы управления | «Секрет Особого Назначения» | Ссылки на документацию |
|---|---|---|---|---|---|
| | | | | При попытке использования на неразрешенных компьютерах «Секрет Особого Назначения» не примонтируется, таким образом, исключаются следующие возможные пути утечки информации:<br>1. копирование пользователем информации конфиденциального характера с компьютера, доступ к которому данному пользователю не разрешен;<br>2. перенос пользователем информации конфиденциального характера с своей рабочей станции на личный компьютер;<br>3. кража информации конфиденциального характера в случае потери специального носителя. | |

Итак, путем применения ПАК «Секрет Особого Назначения» в автоматизированной системе управления выполняются следующие меры, включенные в базовый набор мер защиты информации для соответствующего класса защищенности информационной системы:

ИАФ: 1, 2, 4, 7;

УПД: 1, 2, 4, 5, 6, 9, 11, 14;

ЗНИ: 2, 5, 6, 7, 8;

АУД: 2, 3, 4, 6, 7, 8, 9;

ОЦЛ: 1, 3, 5;

ЗИС: 1, 13, 20, 33;

ИНЦ: 1, 2;

ОПО: 4.

а также дополнительные (не включенные в базовый набор) меры:

ЗНИ; 3, 4;

ОЦЛ: 2;

ЗИС: 10, 12, 14, 17.

ОКБ САПР
www.okbsapr.ru
okbsapr@okbsapr.ru
Россия, 115114, Москва, 2-ой Кожевнический переулок, д. 12
Тел.: +7 (495) 994-72-62