СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

DALLAS LOCK 8.0

РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ

ДЛЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ О ЗАЩИТЕ ИНФОРМАЦИИ

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

DALLAS LOCK 8.0

РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ

ДЛЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ О ЗАЩИТЕ ИНФОРМАЦИИ

СОДЕРЖАНИЕ

РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ
ДЛЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ О ЗАЩИТЕ ИНФОРМАЦИИ

1. ТЕРМИНЫ И СОКРАЩЕНИЯ

АС	автоматизированная система
МЭ	межсетевой экран
НДВ	недекларированные возможности
НСД	несанкционированный доступ
РД	руководящий документ
СБ	Сервер безопасности СЗИ НСД «Dallas Lock»
СДЗ	средство доверенной загрузки
СЗИ ВИ	средство защиты информации в виртуальных инфраструктурах
СКУД	система контроля и управления доступом
СОВ	система обнаружения вторжений
DL 8.0	СЗИ НСД «Dallas Lock 8.0»

2. РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ ДЛЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ О ЗАЩИТЕ ИНФОРМАЦИИ

Dallas Lock 8.0 – сертифицированная система защиты информации накладного типа для автономных и сетевых АРМ (применима для сложных сетевых инфраструктур).

Предназначена для защиты конфиденциальной информации (редакции «К» и «С»), в том числе содержащейся в автоматизированных системах (АС) до класса защищенности 1Г включительно, в государственных информационных системах (ГИС) до 1 класса защищенности включительно, в информационных системах персональных данных (ИСПДн) для обеспечения 1 уровня защищенности ПДн, в автоматизированных системах управления производственными и технологическими процессами (АСУ ТП) до 1 класса защищенности включительно, в значимых объектах критической информационной инфраструктуры (КИИ) до 1 категории включительно, а также для защиты информации, содержащей сведения, составляющие государственную тайну (редакция «С») до уровня «совершенно секретно» включительно.

Использование СЗИ необходимо в соответствии с закрепленными в приказах и руководящих документах регулятора группами мер, которые являются обязательными для выполнения:

- идентификация и аутентификация в информационной системе;
- управление доступом к компонентам информационной системы и информационным ресурсам,
- ограничение программной среды;
- регистрация событий безопасности в информационной системе;
- обеспечение целостности информационной системы и информации.

Указанные группы мер должны быть реализованы в ИСПДн (Приказ ФСТЭК России № 21), в ГИС (Приказ ФСТЭК России № 17), в АСУ ТП (Приказ ФСТЭК России № 31), в КИИ (Приказ ФСТЭК России №239), а также в автоматизированных системах классов 1Д и выше (Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации).

2.1 АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ

СЗИ Dallas Lock, при определенных настройках, обеспечивает соответствие для следующих классов защищенности АС согласно РД «Автоматизированные системы. Защита он несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»:

Группа АС	Классы защищенности				
АС первой группы		1Б	1В	1Г	1Д
АС второй группы	2А	2Б			
АС третьей группы	3А	3Б			

Для соответствия классам защищенности АС должны быть настроены параметры безопасности, перечисленные в таблицах №1, №2, №3, №4.

В таблице №1 представлены политики безопасности категории «Параметры безопасности».
В таблице №2 представлены политики безопасности категории «Контроль ресурсов».
В таблице №3 представлены политики безопасности категории «МЭ».
В таблице №4 представлены политики безопасности категории «СОВ».

Примечание. Условные обозначения

(обяз.)	- действие обязательно для выполнения в соответствии с требованиями
(реком.)	- значение параметра выставлено по умолчанию как рекомендуемое для выполнения, но может быть настроено на усмотрение администратора безопасности
(АИБ)	- значение параметра отключено по умолчанию и может быть настроено на усмотрение администратора безопасности. Пример: *значение по умолчанию (АИБ)*
«-»	- параметр отсутствует (например, из-за отсутствия в параметрах безопасности редакции «К»)

Таблица №1. Политики безопасности вкладки «Параметры безопасности»

Параметры	Классы защищенности АС/Значения параметров		
	1Б, 1В, 1Г, 1Д	**2А, 2Б**	**3А, 3Б**
Категория «Вход»	**Значения параметров**		
Вход: запрет смены пользователя без перезагрузки	1Б: Вкл. (реком.) 1В, 1Г, 1Д: Выкл. (АИБ)	2А: Вкл. (реком.) 2Б: Выкл. (АИБ)	Выкл. (АИБ)
Вход: отображать имя последнего пользователя	Да (реком.)	Да (реком.)	Да (реком.)
Вход: максимальное кол-во ошибок ввода пароля	5 (реком.)	5 (реком.)	5 (реком.)
Вход: время блокировки учетной записи в случае ввода неправильных паролей	15 мин. (реком.)	15 мин. (реком.)	15 мин. (реком.)
Вход: отображать информацию о последнем успешном входе	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)

Продолжение **Таблицы №1**

РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ
ДЛЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ О ЗАЩИТЕ ИНФОРМАЦИИ

Параметры	Классы защищенности АС/Значения параметров		
	1Б, 1В, 1Г, 1Д	2А, 2Б	3А, 3Б
Вход: запрет одновременной работы пользователей с различными уровнями или метками мандатного доступа	1Б, 1В: Выкл. (АИБ) 1Г, 1Д: «-»	2А: Выкл. (АИБ) 2Б: «-»	«-»
Вход: выбор мандатной метки при входе в ОС	1Б, 1В: Выкл. (АИБ) 1Г, 1Д: «-»	2А: Выкл. (АИБ) 2Б: «-»	«-»
Вход: разрешить использование смарт-карт	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Вход: запретить использование парольного интерфейса входа	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Вход: автоматический выбор аппаратного идентификатора при авторизации	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Пароли: максимальный срок действия пароля	42 дн. (реком.)	42 дн. (реком.)	42 дн. (реком.)
Пароли: минимальный срок действия пароля	Не используется (АИБ)	Не используется (АИБ)	Не используется (АИБ)
Пароли: напоминать о смене пароля за	14 дн. (реком.)	14 дн. (реком.)	14 дн. (реком.)
Пароли: минимальная длина	1Б: не менее 8 симв. (обяз.) 1В, 1Г, 1Д: не менее 6 симв. (обяз.)	не менее 6 симв. (обяз.)	не менее 6 симв. (обяз.)
Пароли: необходимо наличие цифр	Да (обяз.)	Да (обяз.)	Да (обяз.)
Пароли: необходимо наличие спец. символов	1Б: Да (реком.) 1В, 1Г, 1Д: Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Пароли: необходимо наличие строчных и прописных букв	1Б: Да (реком.) 1В, 1Г, 1Д: Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Пароли: необходимо отсутствие цифр в первом и последнем символе	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Пароли: необходимо изменение пароля не меньше чем	Не используется (АИБ)	Не используется (АИБ)	Не используется (АИБ)
Домен безопасности	Не задан (АИБ)	Не задан (АИБ)	Не задан (АИБ)
Сеть: Ключ удаленного доступа	АИБ	АИБ	АИБ
Сеть: Время хранения сетевого кэша	30 мин (АИБ)	30 мин (АИБ)	30 мин (АИБ)
Сеть: список незащищенных серверов	АИБ	АИБ	АИБ
Настройка считывателей аппаратных идентификаторов	АИБ	АИБ	АИБ
Блокировать компьютер при отключении аппаратного идентификатора	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Блокировать файл-диски при отключении аппаратного идентификатора	Да (АИБ)	Да (АИБ)	Да (АИБ)
Текс сообщения при входе	АИБ	АИБ	АИБ
Использовать авторизационную информацию от СДЗ Dallas Lock	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Категория «Аудит»	**Значения параметров**		
Журнал входов в систему	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)
Журнал ресурсов	1Д: Вкл. (реком.) 1Г, 1В, 1Б: Вкл. (обяз.)	2А: Вкл. (обяз.) 2Б: Вкл. (реком.)	Вкл. (реком.)
Журнал управления политиками безопасности	1Д, 1Г: Вкл. (реком.) 1В, 1Б: Вкл. (обяз.)	Вкл. (реком.)	Вкл. (реком.)

Продолжение **Таблицы №1**

РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ
ДЛЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ О ЗАЩИТЕ ИНФОРМАЦИИ

Параметры	Классы защищенности АС/Значения параметров		
	1Б, 1В, 1Г, 1Д	2А, 2Б	3А, 3Б
Журнал управления учетными записями	1Д, 1Г: Вкл. (реком.) 1В, 1Б: Вкл. (обяз.)	Вкл. (реком.)	Вкл. (реком.)
Журнал печати	1Д: Выкл. (АИБ) 1Г, 1В, 1Б: Вкл. (обяз.)	2А: Вкл. (обяз.) 2Б: Выкл. (АИБ)	3А: Вкл. (обяз.) 3Б: Выкл. (АИБ)
Журнал запуска/завершения процессов	1Д: Вкл. (реком.) 1Г, 1В, 1Б: Вкл. (обяз.)	2А: Вкл. (обяз.) 2Б: Вкл. (реком.)	Вкл. (реком.)
Служебный журнал МЭ	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Журнал пакетов МЭ	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Журнал соединений МЭ	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Журнал трафика фильтрации МЭ	Вкл. (АИБ)	Вкл. (АИБ)	Вкл. (АИБ)
Журнал событий ОС	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)
Журнал трафика СОВ	Вкл. (АИБ)	Вкл. (АИБ)	Вкл. (АИБ)
Журнал контроля приложений СОВ	Вкл. (АИБ)	Вкл. (АИБ)	Вкл. (АИБ)
Фиксировать в журнале входов неправильные пароли	1Д: Нет (АИБ) 1Г, 1В, 1Б:Да (обяз.)	Нет (АИБ)	Нет (АИБ)
Заносить в журнал исходящие попытки входа на удаленные компьютеры	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Заносить в журнал события запуска и остановки ОС	Да (обяз.)	Да (обяз.)	Да (обяз.)
Заносить в журнал события запуска и остановки модулей администрирования DL	1Д: Да (реком.) 1Г, 1В, 1Д: Да (обяз.)	2А: Вкл. (обяз.) 2Б: Вкл. (реком.)	Вкл. (реком.)
Аудит устройств	1Д: Вкл. (реком.) 1Г, 1В, 1Д: Вкл. (обяз.)	2А: Вкл. (обяз.) 2Б: Вкл. (реком.)	3А: Вкл. (обяз.) 3Б: Вкл. (реком.)
Аудит событий зачистки	1Д: Вкл. (реком.) 1Г, 1В, 1Д: Вкл. (обяз.)	2А: Вкл. (обяз.) 2Б: Вкл. (реком.)	3А: Вкл. (обяз.) 3Б: Вкл. (реком.)
Аудит доступа: Заносить в журналы ошибки ОС	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Аудит доступа/запуска: Вести аудит системных пользователей	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Печатать/редактировать штамп	1Д, 1Г: Нет (АИБ) 1В, 1Б: Да (обяз.)	2А: Да (обяз.) 2Б: Нет (АИБ)	3А: Да (обяз.) 3Б: Нет (АИБ)
Создавать теневые копии распечатываемых документов	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Разрешать печатать из-под уровней доступа	1Д, 1Г: «-» 1В, 1Б: Все уровни (реком.)	2А: Все уровни (реком.) 2Б: «-»	«-»
Добавлять штамп при печати под уровнями	1Д, 1Г: «-» 1В, 1Б: Все уровни (реком.)	2А: Все уровни (реком.) 2Б: «-»	«-»
Выгрузка журналов	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Максимальное кол-во записей в журналах	2 000 (АИБ)	2 000 (АИБ)	2 000 (АИБ)
Периодическая архивация журналов	Не используется (АИБ)	Не используется (АИБ)	Не используется (АИБ)
Категория «Права пользователей»	**Значения параметров**		
Все значения параметров данной категории выставлены по умолчанию как рекомендуемые для выполнения, но могут быть настроены на усмотрение администратора безопасности, в соответствии с требованиями безопасности организации			

Продолжение **Таблицы №1**

Параметры	Классы защищенности АС/Значения параметров		
	1Б, 1В, 1Г, 1Д	2А, 2Б	3А, 3Б
Категория «Мандатный доступ»	**Значения параметров**		
Категория «Мандатный доступ» доступна только для редакции «С», включает в состав подкатегорию «Уровни доступа» и «Мандатные метки». Предоставлено 7 уровней мандатного доступа (начиная с 0), АИБ может переименовывать название уровней и выполнять действия по управлению мандатными метками			
Категория «Очистка остаточной информации»	**Значения параметров**		
Очищать освобождаемое дисковое пространство	1Д: Нет (АИБ) 1Г, 1В, 1Б: Да (обяз.)	2А: Да (обяз.) 2Б: Нет (АИБ)	3А: Да (обяз.) 3Б: Нет (АИБ)
Очищать файл подкачки виртуальной памяти	1Д: Нет (АИБ) 1Г, 1В, 1Б: Да (обяз.)	2А: Да (обяз.) 2Б: Нет (АИБ)	3А: Да (обяз.) 3Б: Нет (АИБ)
Очищать данные в конфиденциальных сеансах доступа	1Д, 1Г: «-» 1В, 1Б: Да (обяз.)	2А: Да (обяз.) 2Б: «-»	«-»
Проверять очистку информации	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Количество циклов затирания	1Д: «1» (требования по количеству циклов затирания к 1Д не предъявляются, по умолчанию выставлено значение «1») 1Г: «1» (как минимум «1» цикл затирания, значение может быть изменено в большую сторону) 1В, 1Б: «2» (как минимум обязательно «2» цикла затирания, значение может быть изменено в большую сторону)	2А: как минимум 2 (обяз.) 2Б: «1» (требования по количеству циклов затирания к 2Б не предъявляются, по умолчанию выставлено значение «1»)	3А: как минимум 2 (обяз.) 3Б: «1» (требования по количеству циклов затирания к 3Б не предъявляются, по умолчанию выставлено значение «1»)
Затирающая последовательность	00 00 00 00 (АИБ)	00 00 00 00 (АИБ)	00 00 00 00 (АИБ)
Категория «Контроль целостности» **Подкатегория «Политики»**	**Значения параметров**		
Проверять целостность ФС при загрузке ОС	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)
Периодический контроль ФС	Не используется (АИБ)	Не используется (АИБ)	Не используется (АИБ)
Контроль ФС по расписанию	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Проверять целостность прогр.апп. среды при загрузке ОС	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)
Периодический контроль прогр. апп. среды	Не используется (АИБ)	Не используется (АИБ)	Не используется (АИБ)
Контроль прогр.апп. среды по расписанию	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Проверять целостность реестра при загрузке ОС	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)
Периодический контроль реестра	Не используется (АИБ)	Не используется (АИБ)	Не используется (АИБ)
Контроль реестра по расписанию	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Изменение файлов с назначенным контролем целостности	Разрешить (реком.)	Разрешить (реком.)	Разрешить (реком.)
Подкатегория «Прогр.апп. среда»	Для параметров данной категории выставлено значение «Выключено», необходимые значения выставляет администратор информационной безопасности самостоятельно		
Категория «Блокируемые расширения»	В данной категории администратор информационной безопасности самостоятельно настраивает список расширений, которые необходимо блокировать		

Продолжение **Таблицы №1**

Параметры	Классы защищенности АС/Значения параметров		
	1Б, 1В, 1Г, 1Д	2А, 2Б	3А, 3Б
Категория «Изолированные процессы»	В данной категории администратор информационной безопасности самостоятельно настраивает список процессов, которые необходимо изолировать/не изолировать. По умолчанию все процессы не изолированы		
Категория «Загрузчик DL»	Категория доступна только для редакции «С» и предназначена для включения и настройки режима загрузчика DL. Модуль загрузчика отрабатывает до загрузки ОС и выполняет роль дополнительного уровня защиты при попытке доступа к компьютеру		

Таблица №2. Политики безопасности вкладки «Контроль ресурсов»

Параметры	Классы защищенности АС/Значения параметров		
	1Б, 1В, 1Г, 1Д	2А, 2Б	3А, 3Б
Значения параметров			
Категория «Дискреционный доступ»	По умолчанию заданы следующие параметры, рекомендуем данные параметры оставить: - Параметры фиксированных дисков по умолчанию - C:\DLLOCK80\Logs - C:\DLLOCK80\Passports Остальные параметры данной категории настраиваются самостоятельно администратором информационной безопасности		
Категория «Мандатный доступ»	Данная категория доступна только для редакции «С». Параметры данной категории настраиваются самостоятельно администратором информационной безопасности		
Категория «Аудит»	В данной категории по умолчанию уже добавлены имена и параметры файлов, рекомендуем их оставить. Остальные параметры данной категории настраиваются самостоятельно администратором информационной безопасности		
Категория «Контроль целостности»	В данной категории по умолчанию уже добавлены имена и параметры файлов, рекомендуем их оставить. Остальные параметры данной категории настраиваются самостоятельно администратором информационной безопасности		
Категория «Глобальные»	Параметры данной категории администратор информационной безопасности настраивает самостоятельно		
Категория «Устройства»	Параметры данной категории администратор информационной безопасности настраивает самостоятельно		

Таблица №3. Политики безопасности вкладки «МЭ»

Параметры	Классы защищенности АС/Значения параметров		
	1Б, 1В, 1Г, 1Д	2А, 2Б	3А, 3Б
Категория «Параметры»	**Значения параметров**		
Доверенные правила МЭ	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Отключать GZIP для анализа HTTP трафика	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Сохранять локальные правила МЭ при синхронизации с СБ	Да (реком.)	Да (реком.)	Да (реком.)
Режим обучения МЭ	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Список разрешенных драйверов протоколов	Выставлено значение по умолчанию «*» (АИБ)	Выставлено значение по умолчанию «*» (АИБ)	Выставлено значение по умолчанию «*» (АИБ)
Протоколирование событий изменения конфигурации	По умолчанию выбраны все события (реком.)	По умолчанию выбраны все события (реком.)	По умолчанию выбраны все события (реком.)
Периодичность проверки защищенности системы	По умолчанию выставлено значение «10 минут»» (АИБ)	По умолчанию выставлено значение «10 минут»» (АИБ)	По умолчанию выставлено значение «10 минут»» (АИБ)
Уведомления по событиям отсутствия антивируса и обновлений ОС и DL	По умолчанию выставлено значение «Уведомление в журнал» (АИБ)	По умолчанию выставлено значение «Уведомление в журнал» (АИБ)	По умолчанию выставлено значение «Уведомление в журнал» (АИБ)

Продолжение **Таблицы №3**

Параметры	Классы защищенности АС/Значения параметров		
	1Б, 1В, 1Г, 1Д	2А, 2Б	3А, 3Б
Отключать локальные правила МЭ при автопереключении профиля МЭ	Да (реком.)	Да (реком.)	Да (реком.)
Порты сторонних программ	Необходимые значения администратор информационной безопасности устанавливает самостоятельно		
Категория «Правила МЭ»	По умолчанию в данную категорию уже добавлен набор правил. Все правила, кроме «Действия с пакетами, не попавшими ни под одно правило», деактивированы. Администратор информационной безопасности может самостоятельно добавить новое правило и активировать его, либо активировать правило по умолчанию. Правило «Действия с пакетами, не попавшими ни под одно правило» рекомендуем оставить в состоянии «Активировано»		
Категория «Профили МЭ»	По умолчанию уже добавлен один профиль. Администратор информационной безопасности может самостоятельно настроить профиль по умолчанию или добавить собственные профили		
Категория «Фильтрация»	**Значения параметров**		
Список перехватываемых исходящих портов	По умолчанию добавлены порты: 80, 443, 3128, 8080, рекомендуем их оставить. Администратор информационной безопасности может самостоятельно дополнять список		
Режим работы	По умолчанию выставлено значение «Фильтровать все, кроем исключений» (реком.)		
Анализ SSL трафика	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Максимальный размер http-заголовка	2048 симв. (АИБ)	2048 симв. (АИБ)	2048 симв. (АИБ)
Включить уведомление в трей при блокировке соединения	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)

Таблица №4. Политики безопасности вкладки «СОВ»

Параметры	Классы защищенности АС/Значения параметров		
	1Б, 1В, 1Г, 1Д	2А, 2Б	3А, 3Б
Значения параметров			
Категория «Сигнатуры»	По умолчанию в категорию уже добавлен набор сигнатур, все они находятся в состоянии «Активировано», рекомендуем их оставить. Администратор информационной безопасности может самостоятельно добавлять сигнатуры журналов		
Категория «Параметры СОВ»	**Значения параметров**		
Подкатегория «Контроль приложений»	По умолчанию в категорию добавлено три правила журнала приложений СОВ. Администратор информационной безопасности может самостоятельно добавить новые правила или редактировать правила по умолчанию		
Подкатегория «Контроль реестра»	Данная категория уже содержит список ключей, находящихся в состоянии «Деактивировано». Администратор информационной безопасности может самостоятельно добавлять новые ключи или активировать ключи по умолчанию		
Подкатегория «Настройки эвристики»	Данная категория уже содержит список атак и настройки эвристики для каждой из них. Рекомендуем оставить все атаки в состоянии «Вкл.» (реагирование на атаки). Администратор информационной безопасности может самостоятельно редактировать настройки эвристики для каждой атаки		
Подкатегория «Глобальные параметры»	**Значения параметров**		
Анализ журналов ОС	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Анализ сигнатур атак в сетевом трафике	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Контроль приложений	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Блокировка атак на протоколы и сканирование	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Не заносить повторы в журнал контроля приложений	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Блокировать снятие скриншотов по клавише PrintScreen	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)

Продолжение **Таблицы №4**

Параметры	Классы защищенности АС/Значения параметров		
	1Б, 1В, 1Г, 1Д	2А, 2Б	3А, 3Б
Расширенное определение атак подмены адресов	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Маскирование датчика СОВ	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
URL обновлений	updates.dallaslock.ru/ Update (обяз.)	updates.dallaslock.ru/ Update (обяз.)	updates.dallaslock.ru/Update (обяз.)
Регулярность обновлений	Раз в сутки (реком.)	Раз в сутки (реком.)	Раз в сутки (реком.)
Заносить в журнал политик проверки наличия обновлений	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Обновление сигнатур журналов	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Обновление детектора атак	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Обновление настроек эвристики	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Обновление сигнатур трафика	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Обновление переменных трафика	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Настройки оповещения контроля приложений	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Настройки списков блокировок	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Категория «Безопасная среда»	**Значения параметров**		
Подкатегория «Настройка»			
Использовать безопасную среда	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Показывать диалог с сохранением изменений после завершения	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Автоматическая очистка по завершении всех процессов	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Эвристический анализ для блокировки работы опасных процессов	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Формировать отчет по завершении работы процессов в БС	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Подкатегория «Контроль приложений»	Данная подкатегория уже содержит правило безопасной среды по умолчанию. Администратор информационной безопасности самостоятельно может настраивать дополнительные правила		
Подкатегория «Файловая система и реестр»	Данная подкатегория уже содержит правило по умолчанию, администратор информационной безопасности может самостоятельно его редактировать		

2.2 ГОСУДАРСТВЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

СЗИ НСД Dallas Lock может быть использовано в государственных информационных системах 1 класса защищенности.

При определенных настройках СЗИ обеспечивает соответствие требованиям для государственных информационных систем (ГИС), представленных в следующих методических документах:
- требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (Приказ ФСТЭК России от 11 февраля 2013 г. №17);
- меры защиты информации в государственных информационных системах (утверждены ФСТЭК России 11 февраля 2014 г.).

Согласно Приказу ФСТЭК России № 17 определяются 3 класса защищенности: К1, К2 и К3. Для классов защищенности устанавливаются базовые наборы мер защиты информации.

Примечание. В системах ГИС классов К1 и К2 должна выполняться доверенная загрузка средств вычислительной техники (мера УПД.17). Для выполнения данного требования может быть использовано средство доверенной загрузки «Dallas Lock» или программный модуль «Загрузчик Dallas Lock» (данный механизм доступен только для редакции «С»). Загрузчик может быть использован в ИС, где угроза недоверенной загрузки не является актуальной или где нерентабельно, или конструктивно невозможно использовать СДЗ уровня платы расширения.

Примечание. Выполнение меры «УПД.9. Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя ИС» выполняется при создании/редактировании учетной записи пользователя в поле «Число разрешенных сеансов». Для ИС класса ИК1 число разрешенных сеансов - не более 2-х.

Примечание. В ИС класса К1 должно выполняться резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы. Для реализации данной меры необходимо использовать функциональную возможность репликации Серверов безопасности «Dallas Lock».

Для соответствия классам защищенности ГИС должны быть настроены параметры безопасности, перечисленные в таблицах №5, №6, №7, №8.
В таблице №5 представлены политики безопасности категории «Параметры безопасности».
В таблице №6 представлены политики безопасности категории «Контроль ресурсов».
В таблице №7 представлены политики безопасности категории «МЭ».
В таблице №8 представлены политики безопасности категории «СОВ».

Примечание. Условные обозначения

(обяз.)	- действие обязательно для выполнения в соответствии с требованиями
(реком.)	- значение параметра выставлено по умолчанию как рекомендуемое для выполнения, но может быть настроено на усмотрение администратора безопасности
(АИБ)	- значение параметра отключено по умолчанию и может быть настроено на усмотрение администратора безопасности. Пример: *значение по умолчанию (АИБ)*
«-»	- параметр отсутствует (например, из-за отсутствия в параметрах безопасности редакции «К»)

Таблица №5. Политики безопасности вкладки «Параметры безопасности»

Параметры	Классы защищенности ИС/Значения параметров		
	К1	К2	К3
Категория «Вход»	**Значения параметров**		
Вход: запрет смены пользователя без перезагрузки	Вкл. (АИБ)	Вкл. (АИБ)	Вкл. (АИБ)
Вход: отображать имя последнего пользователя	Да (реком.)	Да (реком.)	Да (реком.)
Вход: максимальное кол-во ошибок ввода пароля	От 3 до 4 (обяз.)	От 3 до 8 (обяз.)	От 3 до 10 (обяз.)
Вход: время блокировки учетной записи в случае ввода неправильных паролей	От 15 до 60 мин. (обяз.)	От 10 до 30 мин. (обяз.)	От 5 до 30 мин. (обяз.)
Вход: отображать информацию о последнем успешном входе	Да (реком.)	Да (реком.)	Да (реком.)
Вход: запрет одновременной работы пользователей с различными уровнями или метками мандатного доступа	Для редакции «К»: - Для редакции «С»: «Выкл.» (АИБ)	Для редакции «К»: - Для редакции «С»: «Выкл.» (АИБ)	Для редакции «К»: - Для редакции «С»: «Выкл.» (АИБ)
Вход: выбор мандатной метки при входе в ОС	Для редакции «К»: - Для редакции «С»: «Выкл.» (АИБ)	Для редакции «К»: - Для редакции «С»: «Выкл.» (АИБ)	Для редакции «К»: - Для редакции «С»: «Выкл.» (АИБ)
Вход: разрешить использование смарт-карт	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Вход: запретить использование парольного интерфейса входа	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Вход: автоматический выбор аппаратного идентификатора при авторизации	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Пароли: максимальный срок действия пароля	Не более 60 дней (обяз.)	Не более 90 дней (обяз.)	Не более 120 дней (обяз.)
Пароли: минимальный срок действия пароля	От 1 до 30 дней (обяз.)	От 1 до 30 дней (обяз.)	От 1 до 30 дней (обяз.)
Пароли: напоминать о смене пароля за	14 дн. (АИБ)	14 дн. (АИБ)	14 дн. (АИБ)
Пароли: минимальная длина	Не менее 8 симв. (обяз.)	Не менее 6 симв. (обяз.)	Не менее 6 симв. (обяз.)
Пароли: необходимо наличие цифр	Да (обяз.)	Да (обяз.)	Да (обяз.)
Пароли: необходимо наличие спец. символов	Да (обяз.)	Да (обяз.)	Да (обяз.)
Пароли: необходимо наличие строчных и прописных букв	Да (обяз.)	Да (обяз.)	Да (обяз.)
Пароли: необходимо отсутствие цифр в первом и последнем символе	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Пароли: необходимо изменение пароля не меньше чем	От 1 до 10 симв. (обяз.)	От 1 до 10 симв. (обяз.)	От 1 до 10 симв. (обяз.)
Домен безопасности	Заполняется АИБ (обяз.)	Заполняется АИБ (обяз.)	Заполняется АИБ (обяз.)
Сеть: Ключ удаленного доступа	АИБ	АИБ	АИБ
Сеть: Время хранения сетевого кэша	30 мин. (АИБ)	30 мин. (АИБ)	30 мин. (АИБ)
Сеть: список незащищенных серверов	АИБ	АИБ	АИБ

Продолжение **Таблицы №5**

Параметры	Классы защищенности ИС/Значения параметров		
	К1	К2	К3
Настройка считывателей аппаратных идентификаторов	Данный параметр настраивается АИБ, в зависимости от используемых считывателей электронных идентификаторов	Данный параметр настраивается АИБ, в зависимости от используемых считывателей электронных идентификаторов	Данный параметр настраивается АИБ, в зависимости от используемых считывателей электронных идентификаторов
Блокировать компьютер при отключении аппаратного идентификатора	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Блокировать файл-диски при отключении аппаратного идентификатора	Да (реком.)	Да (реком.)	Да (реком.)
Текст сообщения при входе	Рекомендуем установить	Рекомендуем установить	Рекомендуем установить
Использовать авторизационную информацию от СДЗ Dallas Lock	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Категория «Аудит»	**Значения параметров**		
Журнал входов в систему	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)
Журнал ресурсов	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)
Журнал управления политиками безопасности	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)
Журнал управления учетными записями	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)
Журнал печати	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Журнал запуска/завершения процессов	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)
Служебный журнал МЭ	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Журнал пакетов МЭ	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Журнал соединений МЭ	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Журнал трафика фильтрации МЭ	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)
Журнал событий ОС	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)
Журнал трафика СОВ	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Журнал контроля приложений СОВ	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)
Фиксировать в журнале входов неправильные пароли	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)А
Заносить в журнал исходящие попытки входа на удаленные компьютеры	Да (реком.)	Да (реком.)	Да (реком.)
Заносить в журнал события запуска и остановки ОС	Да (обяз.)	Да (обяз.)	Да (обяз.)
Заносить в журнал события запуска и остановки модулей администрирования DL	Да (реком.)	Да (реком.)	Да (реком.)
Аудит устройств	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)
Аудит событий зачистки	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Аудит доступа: Заносить в журналы ошибки ОС	Вкл. (обяз.)	Выкл. (АИБ)	Выкл. (АИБ)
Аудит доступа/запуска: Вести аудит системных пользователей	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Печатать/редактировать штамп	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Создавать теневые копии распечатываемых документов	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Разрешать печатать из-под уровней доступа	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Добавлять штамп при печати под уровнями	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)

Продолжение **Таблицы №5**

Параметры	Классы защищенности ИС/Значения параметров		
	К1	К2	К3
Выгрузка журналов	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Максимальное кол-во записей в журналах	Значение устанавливается АИБ	Значение устанавливается АИБ	Значение устанавливается АИБ
Периодическая архивация журналов	Не менее 3 мес. (обяз.)	Не менее 3 мес. (обяз.)	Не менее 3 мес. (обяз.)
Категория «Права пользователей»	**Значения параметров**		
Все значения параметров данной категории выставлены по умолчанию как рекомендуемые для выполнения, но могут быть настроены на усмотрение администратора безопасности, в соответствии с требованиями безопасности организации			
Категория «Мандатный доступ»	**Значения параметров**		
Категория «Мандатный доступ» доступна только для редакции «С», включает в состав подкатегорию «Уровни доступа» и «Мандатные метки». Предоставлено 7 уровней мандатного доступа (начиная с 0), АИБ может переименовывать название уровней и выполнять действия по управлению мандатными метками			
Категория «Очистка остаточной информации»	**Значения параметров**		
Очищать освобождаемое дисковое пространство	Да (реком.)	Да (реком.)	Да (реком.)
Очищать файл подкачки виртуальной памяти	Да (реком.)	Да (реком.)	Да (реком.)
Очищать данные в конфиденциальных сеансах доступа	Да (реком.)	Да (реком.)	Да (реком.)
Проверять очистку информации	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Количество циклов затирания	От 1 (АИБ)	От 1 (АИБ)	От 1 (АИБ)
Затирающая последовательность	Значение выставляется АИБ	Значение выставляется АИБ	Значение выставляется АИБ
Категория «Контроль целостности»	**Значения параметров**		
Подкатегория «Политики»			
Проверять целостность ФС при загрузке ОС	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)
Периодический контроль ФС	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ
Контроль ФС по расписанию	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ
Проверять целостность прогр. апп. среды при загрузке ОС	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)
Периодический контроль прогр. апп. среды	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ
Контроль прогр.апп. среды по расписанию	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ
Проверять целостность реестра при загрузке ОС	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)
Периодический контроль реестра	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ

Продолжение **Таблицы №5**

Параметры	Классы защищенности ИС/Значения параметров		
	К1	К2	К3
Контроль реестра по расписанию	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ
Изменение файлов с назначенным контролем целостности	Разрешать (АИБ)	Разрешать (АИБ)	Разрешать (АИБ)
Подкатегория «Прогр.апп. среда»	Для параметров данной категории выставлено значение «Выключено», необходимые значения выставляет администратор информационной безопасности самостоятельно		
Категория «Блокируемые расширения»	В данной категории администратор информационной безопасности самостоятельно настраивает список расширений, которые необходимо блокировать		
Категория «Изолированные процессы»	В данной категории администратор информационной безопасности самостоятельно настраивает список процессов, которые необходимо изолировать/не изолировать. По умолчанию все процессы не изолированы		
Категория «Загрузчик DL»	Категория доступна только для редакции «С» и предназначена для включения и настройки режима загрузчика DL. Модуль загрузчика отрабатывает до загрузки ОС и выполняет роль дополнительного уровня защиты при попытке доступа к компьютеру		

Таблица №6. Политики безопасности вкладки «Контроль ресурсов»

Параметры	Классы защищенности ГИС/Значения параметров		
	К1	К2	К3
Значения параметров			
Категория «Дискреционный доступ»	По умолчанию заданы следующие параметры, рекомендуем данные параметры оставить: - Параметры фиксированных дисков по умолчанию - C:\DLLOCK80\Logs - C:\DLLOCK80\Passports Остальные параметры данной категории настраиваются самостоятельно администратором информационной безопасности		
Категория «Мандатный доступ»	Данная категория доступна только для редакции «С». Параметры данной категории настраиваются самостоятельно администратором информационной безопасности		
Категория «Аудит»	В данной категории по умолчанию уже добавлены имена и параметры файлов, рекомендуем их оставить. Остальные параметры данной категории настраиваются самостоятельно администратором информационной безопасности		
Категория «Контроль целостности»	В данной категории по умолчанию уже добавлены имена и параметры файлов, рекомендуем их оставить. Остальные параметры данной категории настраиваются самостоятельно администратором информационной безопасности		
Категория «Глобальные»	Параметры данной категории администратор информационной безопасности настраивает самостоятельно		
Категория «Устройства»	Параметры данной категории администратор информационной безопасности настраивает самостоятельно		

Таблица №7. Политики безопасности вкладки «МЭ»

Параметры	Классы защищенности ИС/Значения параметров		
	К1	К2	К3
Категория «Параметры»	**Значения параметров**		
Доверенные правила МЭ	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Отключать GZIP для анализа HTTP трафика	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Сохранять локальные правила МЭ при синхронизации с СБ	Да (реком.)	Да (реком.)	Да (реком.)
Режим обучения МЭ	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)

Продолжение **Таблицы №7**

Параметры	Классы защищенности ИС/Значения параметров		
	К1	К2	К3
Список разрешенных драйверов протоколов	Выставлено значение по умолчанию «*» (АИБ)	Выставлено значение по умолчанию «*» (АИБ)	Выставлено значение по умолчанию «*» (АИБ)
Протоколирование событий изменения конфигурации	По умолчанию выбраны все события (реком.)	По умолчанию выбраны все события (реком.)	По умолчанию выбраны все события (реком.)
Периодичность проверки защищенности системы	По умолчанию выставлено значение «10 минут»» (АИБ)	По умолчанию выставлено значение «10 минут»» (АИБ)	По умолчанию выставлено значение «10 минут»» (АИБ)
Уведомления по событиям отсутствия антивируса и обновлений ОС и DL	По умолчанию выставлено значение «Уведомление в журнал» (АИБ)	По умолчанию выставлено значение «Уведомление в журнал» (АИБ)	По умолчанию выставлено значение «Уведомление в журнал» (АИБ)
Отключать локальные правила МЭ при автопереключении профиля МЭ	Да (реком.)	Да (реком.)	Да (реком.)
Порты сторонних программ	Необходимые значения администратор информационной безопасности устанавливает самостоятельно		
Категория «Правила МЭ»	По умолчанию в данную категорию уже добавлен набор правил. Все правила, кроме «Действия с пакетами, не попавшими ни под одно правило», деактивированы. Администратор информационной безопасности может самостоятельно добавить новое правило и активировать его, либо активировать правило по умолчанию. Правило «Действия с пакетами, не попавшими ни под одно правило» рекомендуем оставить в состоянии «Активировано»		
Категория «Профили МЭ»	По умолчанию уже добавлен один профиль. Администратор информационной безопасности может самостоятельно настроить профиль по умолчанию или добавить собственные профили		
Категория «Фильтрация»	**Значения параметров**		
Список перехватываемых исходящих портов	По умолчанию добавлены порты: 80, 443, 3128, 8080, рекомендуем их оставить. Администратор информационной безопасности может самостоятельно дополнять список		
Режим работы	По умолчанию выставлено значение «Фильтровать все, кроем исключений» (реком.)		
Анализ SSL трафика	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Максимальный размер http-заголовка	2048 симв. (АИБ)	2048 симв. (АИБ)	2048 симв. (АИБ)
Включить уведомление в трей при блокировке соединения	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)

Таблица №8. Политики безопасности вкладки «СОВ»

Параметры	Классы защищенности ИС/Значения параметров		
	К1	К2	К3
Значения параметров			
Категория «Сигнатуры»	По умолчанию в категорию уже добавлен набор сигнатур, все они находятся в состоянии «Активировано», рекомендуем их оставить. Администратор информационной безопасности может самостоятельно добавлять сигнатуры журналов		
Категория «Параметры СОВ»	**Значения параметров**		
Подкатегория «Контроль приложений»	По умолчанию в категорию добавлено три правила журнала приложений СОВ. Администратор информационной безопасности может самостоятельно добавить новые правила или редактировать правила по умолчанию		
Подкатегория «Контроль реестра»	Данная категория уже содержит список ключей, находящихся в состоянии «Деактивировано». Администратор информационной безопасности может самостоятельно добавлять новые ключи или активировать ключи по умолчанию		
Подкатегория «Настройки эвристики»	Данная категория уже содержит список атак и настройки эвристики для каждой из них. Рекомендуем оставить все атаки в состоянии «Вкл.» (реагирование на атаки). Администратор информационной безопасности может самостоятельно редактировать настройки эвристики для каждой атаки		

Продолжение **Таблицы №8**

РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ
ДЛЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ О ЗАЩИТЕ ИНФОРМАЦИИ

Параметры	Классы защищенности ИС/Значения параметров		
	К1	К2	К3
Подкатегория «Глобальные параметры»	**Значения параметров**		
Анализ журналов ОС	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)
Анализ сигнатур атак в сетевом трафике	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)
Контроль приложений	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)
Блокировка атак на протоколы и сканирование	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)
Не заносить повторы в журнал контроля приложений	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Блокировать снятие скриншотов по клавише PrintScreen	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Расширенное определение атак подмены адресов	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Маскирование датчика СОВ	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
URL обновлений	updates.dallaslock.ru/Update (обяз.)	updates.dallaslock.ru/Update (обяз.)	updates.dallaslock.ru/Update (обяз.), в случае использования обновлений
Регулярность обновлений	Раз в сутки (реком.)	Раз в сутки (реком.)	Раз в сутки (реком.)
Заносить в журнал политик проверки наличия обновлений	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Обновление сигнатур журналов	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)
Обновление детектора атак	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)
Обновление настроек эвристики	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)
Обновление сигнатур трафика	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)
Обновление переменных трафика	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)
Настройки оповещения контроля приложений	Список настраивается АИБ	Список настраивается АИБ	Список настраивается АИБ
Настройки списков блокировок	Список настраивается АИБ	Список настраивается АИБ	Список настраивается АИБ
Категория «Безопасная среда»	**Значения параметров**		
Подкатегория «Настройка»			
Использовать безопасную среду	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Показывать диалог с сохранением изменений после завершения	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Автоматическая очистка по завершении всех процессов	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Эвристический анализ для блокировки работы опасных процессов	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Формировать отчет по завершении работы процессов в БС	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Подкатегория «Контроль приложений»	Данная подкатегория уже содержит правило безопасной среды по умолчанию. Администратор информационной безопасности самостоятельно может настраивать дополнительные правила		
Подкатегория «Файловая система и реестр»	Данная подкатегория уже содержит правило по умолчанию, администратор информационной безопасности может самостоятельно его редактировать		

2.3 ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

СЗИ НСД Dallas Lock может быть использовано в информационных системах персональных данных (ИСПДн) для обеспечения 1 уровня защищенности ПДн.
При определенных настройках СЗИ обеспечивает соответствие требованиям для информационных систем персональных данных (ИСПДн), представленных в следующих методических документах:
- состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Приказ ФСТЭК России от 18 февраля 2013 г. №21).
Согласно Приказу ФСТЭК России № 21 определяются 4 уровня защищенности персональных данных.

Примечание. В системах ИСПДн уровней 1 и 2 должна выполняться доверенная загрузка средств вычислительной техники (мера УПД.17). Для выполнения данного требования может быть использовано средство доверенной загрузки «Dallas Lock» или использовать программный модуль «Загрузчик Dallas Lock» (данный механизм доступен только для редакции «С»). Загрузчик может быть использован в ИСПДн, где угроза недоверенной загрузки не является актуальной или где нерентабельно, или конструктивно невозможно использовать СДЗ уровня платы расширения.

Примечание. В ИСПДн уровня 1 должно выполняться резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы. Для реализации данной меры необходимо использовать функциональную возможность репликации Серверов безопасности «Dallas Lock».

Для соответствия уровням защищенности персональных данных должны быть настроены параметры безопасности, перечисленные в таблицах №9, №10, №11, №12.

В таблице №9 представлены политики безопасности категории «Параметры без-опасности».

В таблице №10 представлены политики безопасности категории «Контроль ресурсов».
В таблице №11 представлены политики безопасности категории «МЭ».
В таблице №12 представлены политики безопасности категории «СОВ».

Примечание. Условные обозначения

(обяз.)	- действие обязательно для выполнения в соответствии с требованиями
(реком.)	- значение параметра выставлено по умолчанию как рекомендуемое для выполнения, но может быть настроено на усмотрение администратора безопасности
(АИБ)	- значение параметра отключено по умолчанию и может быть настроено на усмотрение администратора безопасности. Пример: *значение по умолчанию (АИБ)*
«-»	- параметр отсутствует (например, из-за отсутствия в параметрах безопасности редакции «К»)

Таблица №9. Политики безопасности вкладки «Параметры безопасности»

Параметры	**Уровни защищенности ИСПДн/Значения параметров**			
	1	**2**	**3**	**4**
Категория «Вход»	**Значения параметров**			
Вход: запрет смены пользователя без перезагрузки	Вкл. (АИБ)	Вкл. (АИБ)	Вкл. (АИБ)	Вкл. (АИБ)
Вход: отображать имя последнего пользователя	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)

Продолжение **Таблицы №9**

РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ
ДЛЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ О ЗАЩИТЕ ИНФОРМАЦИИ

Параметры	Уровни защищенности ИСПДн/Значения параметров			
	1	2	3	4
Вход: максимальное кол-во ошибок ввода пароля	От 3 до 4 (обяз.)	От 3 до 8 (обяз.)	От 3 до 10 (обяз.)	От 3 до 10 (обяз.)
Вход: время блокировки учетной записи в случае ввода неправильных паролей	От 15 до 60 мин. (обяз.)	От 10 до 30 мин. (обяз.)	От 5 до 30 мин. (обяз.)	От 3 до 15 мин. (обяз.)
Вход: отображать информацию о последнем успешном входе	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Вход: запрет одновременной работы пользователей с различными уровнями или метками мандатного доступа	Для редакции «К»: - Для редакции «С»: «Выкл.» (АИБ)	Для редакции «К»: - Для редакции «С»: «Выкл.» (АИБ)	Для редакции «К»: - Для редакции «С»: «Выкл.» (АИБ)	Для редакции «К»: - Для редакции «С»: «Выкл.» (АИБ)
Вход: выбор мандатной метки при входе в ОС	Для редакции «К»: - Для редакции «С»: «Выкл.» (АИБ)	Для редакции «К»: - Для редакции «С»: «Выкл.» (АИБ)	Для редакции «К»: - Для редакции «С»: «Выкл.» (АИБ)	Для редакции «К»: - Для редакции «С»: «Выкл.» (АИБ)
Вход: разрешить использование смарт-карт	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Вход: запретить использование парольного интерфейса входа	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Вход: автоматический выбор аппаратного идентификатора при авторизации	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Пароли: максимальный срок действия пароля	Не более 60 дней (обяз.)	Не более 90 дней (обяз.)	Не более 120 дней (обяз.)	Не более 180 дней (обяз.)
Пароли: минимальный срок действия пароля	От 1 до 30 дней (обяз.)	От 1 до 30 дней (обяз.)	От 1 до 30 дней (обяз.)	От 1 до 30 дней (обяз.)
Пароли: напоминать о смене пароля за	14 дн. (АИБ)	14 дн. (АИБ)	14 дн. (АИБ)	14 дн. (АИБ)
Пароли: минимальная длина	Не менее 8 симв. (обяз.)	Не менее 6 симв. (обяз.)	Не менее 6 симв. (обяз.)	Не менее 6 симв. (обяз.)
Пароли: необходимо наличие цифр	Да (обяз.)	Да (обяз.)	Да (обяз.)	Да (обяз.)
Пароли: необходимо наличие спец. символов	Да (обяз.)	Да (обяз.)	Да (обяз.)	Да (обяз.)
Пароли: необходимо наличие строчных и прописных букв	Да (обяз.)	Да (обяз.)	Да (обяз.)	Да (обяз.)
Пароли: необходимо отсутствие цифр в первом и последнем символе	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Пароли: необходимо изменение пароля не меньше чем	От 1 до 10 симв. (обяз.)	От 1 до 10 симв. (обяз.)	От 1 до 10 симв. (обяз.)	От 1 до 10 симв. (обяз.)
Домен безопасности	Заполняется АИБ (обяз.)	Заполняется АИБ (обяз.)	Заполняется АИБ (обяз.)	Заполняется АИБ (обяз.)
Сеть: Ключ удаленного доступа	АИБ	АИБ	АИБ	АИБ
Сеть: Время хранения сетевого кэша	30 мин. (АИБ)	30 мин. (АИБ)	30 мин. (АИБ)	30 мин. (АИБ)
Сеть: список незащищенных серверов	АИБ	АИБ	АИБ	АИБ
Настройка считывателей аппаратных идентификаторов	Данный параметр настрастраивается АИБ, в зависимости от используемых считывателей электронных идентификаторов	Данный параметр настраивается АИБ, в зависимости от используемых считывателей электронных идентификаторов	Данный параметр настраивается АИБ, в зависимости от используемых считывателей электронных идентификаторов	Данный параметр настраивается АИБ, в зависимости от используемых считывателей электронных идентификаторов
Блокировать компьютер при отключении аппаратного идентификатора	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Блокировать файл-диски при отключении аппаратного идентификатора	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)

Продолжение **Таблицы №9**

РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ
ДЛЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ О ЗАЩИТЕ ИНФОРМАЦИИ

Параметры	Уровни защищенности ИСПДн/Значения параметров			
	1	2	3	4
Текст сообщения при входе	Рекомендуем установить	Рекомендуем установить	Рекомендуем установить	Рекомендуем установить
Использовать авторизационную информацию от СДЗ Dallas Lock	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Категория «Аудит»	**Значения параметров**			
Журнал входов в систему	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)
Журнал ресурсов	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)
Журнал управления политиками безопасности	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)	Вкл. (реком.)
Журнал управления учетными записями	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)	Вкл. (реком.)
Журнал печати	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Журнал запуска/завершения процессов	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)
Служебный журнал МЭ	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Журнал пакетов МЭ	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Журнал соединений МЭ	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Журнал трафика фильтрации МЭ	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)
Журнал событий ОС	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)
Журнал трафика СОВ	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Журнал контроля приложений СОВ	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)
Фиксировать в журнале входов неправильные пароли	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Заносить в журнал исходящие попытки входа на удаленные компьютеры	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Заносить в журнал события запуска и остановки ОС	Да (обяз.)	Да (обяз.)	Да (обяз.)	Да (обяз.)
Заносить в журнал события запуска и остановки модулей администрирования DL	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Аудит устройств	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)
Аудит событий зачистки	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Аудит доступа: Заносить в журналы ошибки ОС	Вкл. (обяз.)	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Аудит доступа/запуска: Вести аудит системных пользователей	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Печатать/редактировать штамп	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Создавать теневые копии распечатываемых документов	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Разрешать печатать из-под уровней доступа	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Добавлять штамп при печати под уровнями	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Выгрузка журналов	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Максимальное кол-во записей в журналах	Значение устанавливается АИБ	Значение устанавливается АИБ	Значение устанавливается АИБ	Значение устанавливается АИБ
Периодическая архивация журналов	Не менее 3 мес. (обяз.)	Не менее 3 мес. (обяз.)	Не менее 3 мес. (обяз.)	Не менее 3 мес. (обяз.)
Категория «Права пользователей»	**Значения параметров**			
Все значения параметров данной категории выставлены по умолчанию как рекомендуемые для выполнения, но могут быть настроены на усмотрение администратора безопасности, в соответствии с требованиями безопасности организации				

Продолжение **Таблицы №9**

Параметры	Уровни защищенности ИСПДн/Значения параметров			
	1	2	3	4
Категория «Мандатный доступ»	**Значения параметров**			
Категория «Мандатный доступ» доступна только для редакции «С», включает в состав подкатегорию «Уровни доступа» и «Мандатные метки». Предоставлено 7 уровней мандатного доступа (начиная с 0), АИБ может переименовывать название уровней и выполнять действия по управлению мандатными метками				
Категория «Очистка остаточной информации»	**Значения параметров**			
Очищать освобождаемое дисковое пространство	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Очищать файл подкачки виртуальной памяти	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Очищать данные в конфиденциальных сеансах доступа	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Проверять очистку информации	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Количество циклов затирания	От 1 (АИБ)	От 1 (АИБ)	От 1 (АИБ)	От 1 (АИБ)
Затирающая последовательность	Значение выставляется АИБ	Значение выставляется АИБ	Значение выставляется АИБ	
Категория «Контроль целостности» **Подкатегория «Политики»**	**Значения параметров**			
Проверять целостность ФС при загрузке ОС	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)	Вкл. (реком.)
Периодический контроль ФС	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)	Вкл. (реком.)
Контроль ФС по расписанию	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ
Проверять целостность прогр. апп. среды при загрузке ОС	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)	Вкл. (реком.)
Периодический контроль прогр. апп. среды	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)	Вкл. (реком.)
Контроль прогр.апп. среды по расписанию	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ
Проверять целостность реестра при загрузке ОС	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)	Вкл. (реком.)
Периодический контроль реестра	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)	Вкл. (реком.)
Контроль реестра по расписанию	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ
Изменение файлов с назначенным контролем целостности	Разрешать (АИБ)	Разрешать (АИБ)	Разрешать (АИБ)	Разрешать (АИБ)
Подкатегория «Прогр.апп. среда»	Для параметров данной категории выставлено значение «Выключено», необходимые значения выставляет администратор информационной безопасности самостоятельно			
Категория «Блокируемые расширения»	В данной категории администратор информационной безопасности самостоятельно настраивает список расширений, которые необходимо блокировать			
Категория «Изолированные процессы»	В данной категории администратор информационной безопасности самостоятельно настраивает список процессов, которые необходимо изолировать/не изолировать. По умолчанию все процессы не изолированы			

Продолжение **Таблицы №9**

Параметры	Уровни защищенности ИСПДн/Значения параметров			
	1	2	3	4
Категория «Загрузчик DL»	Категория доступна только для редакции «С» и предназначена для включения и настройки режима загрузчика DL. Модуль загрузчика отрабатывает до загрузки ОС и выполняет роль дополнительного уровня защиты при попытке доступа к компьютера			

Таблица №10. Политики безопасности вкладки «Контроль ресурсов»

Параметры	Уровни защищенности ИСПДн/Значения параметров			
	1	2	3	4
Значения параметров				
Категория «Дискреционный доступ»	По умолчанию заданы следующие параметры, рекомендуем данные параметры оставить: - Параметры фиксированных дисков по умолчанию - C:\DLLOCK80\Logs - C:\DLLOCK80\Passports Остальные параметры данной категории настраиваются самостоятельно администратором информационной безопасности			
Категория «Мандатный доступ»	Данная категория доступна только для редакции «С». Параметры данной категории настраиваются самостоятельно администратором информационной безопасности			
Категория «Аудит»	В данной категории по умолчанию уже добавлены имена и параметры файлов, рекомендуем их оставить. Остальные параметры данной категории настраиваются самостоятельно администратором информационной безопасности			
Категория «Контроль целостности»	В данной категории по умолчанию уже добавлены имена и параметры файлов, рекомендуем их оставить. Остальные параметры данной категории настраиваются самостоятельно администратором информационной безопасности			
Категория «Глобальные»	Параметры данной категории администратор информационной безопасности настраивает самостоятельно			
Категория «Устройства»	Параметры данной категории администратор информационной безопасности настраивает самостоятельно			

Таблица №11. Политики безопасности вкладки «МЭ»

Параметры	Уровни защищенности ИСПДн/Значения параметров			
	1	2	3	4
Категория «Параметры»	**Значения параметров**			
Доверенные правила МЭ	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Отключать GZIP для анализа HTTP трафика	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Сохранять локальные правила МЭ при синхронизации с СБ	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Режим обучения МЭ	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Список разрешенных драйверов протоколов	Выставлено значение по умолчанию «*» (АИБ)	Выставлено значение по умолчанию «*» (АИБ)	Выставлено значение по умолчанию «*» (АИБ)	Выставлено значение по умолчанию «*» (АИБ)
Протоколирование событий изменения конфигурации	По умолчанию выбраны все события (реком.)	По умолчанию выбраны все события (реком.)	По умолчанию выбраны все события (реком.)	По умолчанию выбраны все события (реком.)
Периодичность проверки защищенности системы	По умолчанию выставлено значение «10 минут»» (АИБ)	По умолчанию выставлено значение «10 минут»» (АИБ)	По умолчанию выставлено значение «10 минут»» (АИБ)	По умолчанию выставлено значение «10 минут»» (АИБ)
Уведомления по событиям отсутствия антивируса и обновлений ОС и DL	По умолчанию выставлено значение «Уведомление в журнал» (АИБ)	По умолчанию выставлено значение «Уведомление в журнал» (АИБ)	По умолчанию выставлено значение «Уведомление в журнал» (АИБ)	По умолчанию выставлено значение «Уведомление в журнал» (АИБ)

Продолжение **Таблицы №11**

Параметры	Уровни защищенности ИСПДн/Значения параметров			
	1	2	3	4
Отключать локальные правила МЭ при автопереключении профиля МЭ	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Порты сторонних программ	Необходимые значения администратор информационной безопасности устанавливает самостоятельно			
Категория «Правила МЭ»	По умолчанию в данную категорию уже добавлен набор правил. Все правила, кроме «Действия с пакетами, не попавшими ни под одно правило», деактивированы. Администратор информационной безопасности может самостоятельно добавить новое правило и активировать его, либо активировать правило по умолчанию. Правило «Действия с пакетами, не попавшими ни под одно правило» рекомендуем оставить с состоянии «Активировано»			
Категория «Профили МЭ»	По умолчанию уже добавлен один профиль. Администратор информационной безопасности может самостоятельно настроить профиль по умолчанию или добавить собственные профили			
Категория «Фильтрация»	**Значения параметров**			
Список перехватываемых исходящих портов	По умолчанию добавлены порты: 80, 443, 3128, 8080, рекомендуем их оставить. Администратор информационной безопасности может самостоятельно дополнять список			
Режим работы	По умолчанию выставлено значение «Фильтровать все, кроем исключений» (реком.)			
Анализ SSL трафика	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Максимальный размер http-заголовка	2048 симв. (АИБ)	2048 симв. (АИБ)	2048 симв. (АИБ)	2048 симв. (АИБ)
Включить уведомление в трей при блокировке соединения	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)

Таблица №12. Политики безопасности вкладки «СОВ»

Параметры	Уровни защищенности ИСПДн /Значения параметров			
	1	2	3	4
Значения параметров				
Категория «Сигнатуры»	По умолчанию в категорию уже добавлен набор сигнатур, все они находятся в состоянии «Активировано», рекомендуем их оставить. Администратор информационной безопасности может самостоятельно добавлять сигнатуры журналов			
Категория «Параметры СОВ»	**Значения параметров**			
Подкатегория «Контроль приложений»	По умолчанию в категорию добавлено три правила журнала приложений СОВ. Администратор информационной безопасности может самостоятельно добавить новые правила или редактировать правила по умолчанию			
Подкатегория «Контроль реестра»	Данная категория уже содержит список ключей, находящихся в состоянии «Деактивировано». Администратор информационной безопасности может самостоятельно добавлять новые ключи или активировать ключи по умолчанию			
Подкатегория «Настройки эвристики»	Данная категория уже содержит список атак и настройки эвристики для каждой из них. Рекомендуем оставить все атаки в состоянии «Вкл.» (реагирование на атаки). Администратор информационной безопасности может самостоятельно редактировать настройки эвристики для каждой атаки			
Подкатегория «Глобальные параметры»	**Значения параметров**			
Анализ журналов ОС	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)	Вкл. (реком.)
Анализ сигнатур атак в сетевом трафике	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)	Вкл. (реком.)
Контроль приложений	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)	Вкл. (реком.)
Блокировка атак на протоколы и сканирование	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)	Вкл. (реком.)
Не заносить повторы в журнал контроля приложений	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)

Продолжение **Таблицы №12**

РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ
ДЛЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ О ЗАЩИТЕ ИНФОРМАЦИИ

Параметры	Уровни защищенности ИСПДн /Значения параметров			
	1	2	3	4
Блокировать снятие скриншотов по клавише PrintScreen	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Расширенное определение атак подмены адресов	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Маскирование датчика СОВ	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
URL обновлений	updates.dallaslock.ru/Update (обяз.)	updates.dallaslock.ru/Update (обяз.)	updates.dallaslock.ru/Update (обяз.), в случае использования обновлений	updates.dallaslock.ru/Update (обяз.), в случае использования обновлений
Регулярность обновлений	Раз в сутки (реком.)	Раз в сутки (реком.)	Раз в сутки (реком.)	Раз в сутки (реком.)
Заносить в журнал политик проверки наличия обновлений	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Обновление сигнатур журналов	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)	Вкл. (реком.)
Обновление детектора атак	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)	Вкл. (реком.)
Обновление настроек эвристики	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)	Вкл. (реком.)
Обновление сигнатур трафика	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)	Вкл. (реком.)
Обновление переменных трафика	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (реком.)	Вкл. (реком.)
Настройки оповещения контроля приложений	Список настраивается АИБ	Список настраивается АИБ	Список настраивается АИБ	Список настраивается АИБ
Настройки списков блокировок	Список настраивается АИБ	Список настраивается АИБ	Список настраивается АИБ	Список настраивается АИБ
Категория «Безопасная среда» **Подкатегория «Настройка»**	**Значения параметров**			
Использовать безопасную среду	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Показывать диалог с сохранением изменений после завершения	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Автоматическая очистка по завершению всех процессов	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)	Вкл. (реком.)
Эвристический анализ для блокировки работы опасных процессов	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Формировать отчет по завершении работы процессов в БС	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Подкатегория «Контроль приложений»	Данная подкатегория уже содержит правило безопасной среды по умолчанию. Администратор информационной безопасности самостоятельно может настраивать дополнительные правила			
Подкатегория «Файловая система и реестр»	Данная подкатегория уже содержит правило по умолчанию, администратор информационной безопасности может самостоятельно его редактировать			

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

192029, г. Санкт-Петербург
пр. Обуховской Обороны, д. 51, лит. К
телефон/факс: (812) **325-1037**

http://www.**confident**.ru/
http://www.**dallaslock**.ru/
e-mail:
isc@confident.ru - коммерческие вопросы
helpdesk@confident.ru - техническая поддержка

Схема проезда: