СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

# DALLAS LOCK LINUX

## РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ

ДЛЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ О ЗАЩИТЕ ИНФОРМАЦИИ

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

# DALLAS LOCK LINUX

# РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ

## ДЛЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ О ЗАЩИТЕ ИНФОРМАЦИИ

## СОДЕРЖАНИЕ

# РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ
ДЛЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ О ЗАЩИТЕ ИНФОРМАЦИИ

## ТЕРМИНЫ И СОКРАЩЕНИЯ

| | |
|---|---|
| **АС** | Автоматизированная система |
| **АСУ ТП** | Автоматизированная система управления производственными и технологическими процессами |
| **ГИС** | Государственная информационная система |
| **ИС** | Информационная система |
| **ИСПДн** | Информационная система персональных данных |
| **КИИ** | Критическая информационная структура |
| **СДЗ** | Средство доверенной загрузки |
| **СЗИ НСД** | Система защиты информации от несанкционированного доступа |

## РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ

СЗИ НСД Dallas Lock Linux предназначена для комплексной и многофункциональной защиты информационных ресурсов от несанкционированного доступа при работе в многопользовательских АС до класса защищенности 1Г включительно, ИСПДн для обеспечения 1 уровня защищенности ПДн, АСУ ТП до 1 класса защищенности включительно, ГИС до 1 класса защищенности включительно и при защите значимых объектов КИИ до 1 категории 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,
- регистрация событий безопасности в информационной системе;
- обеспечение целостности информационной системы и информации.

## 1. АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ

При определенных настройках СЗИ НСД Dallas Lock Linux обеспечивает соответствие следующих классов защищенности АС требованиям РД «Автоматизированные системы. Защита он несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Для соответствия классам защищенности АС должны быть настроены параметры безопасности, перечисленные в таблицах 1–6.

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.

**Таблица 1**

| **Параметры** | **Класс защищенности** | | |
|---|---|---|---|
| | **1Б, 1В, 1Г, 1Д** | **2А, 2Б** | **3А, 3Б** |
| **Категория «Настройка сессий»** | **Значения параметров** | | |
| **Максимальное количество сессий** | 10 (АИБ) | 10 (АИБ) | 10 (АИБ) |
| **Таймаут блокировки сессий (в минутах)** | 2 (АИБ) | 2 (АИБ) | 2 (АИБ) |

**Таблица 2**

| Параметры | Класс защищенности | | |
|---|---|---|---|
| | 1Б, 1В, 1Г, 1Д | 2А, 2Б | 3А, 3Б |
| **Категория «Настройка аудита»** | **Значения параметров** | | |
| Срок хранения журналов. Установка срока хранения журналов (в месяцах) | 3 (реком.) | 3 (реком.) | 3 (реком.) |
| Журнал входов/выходов | Вкл. (обяз.) | Вкл. (обяз.) | Вкл. (обяз.) |
| Журнал доступа к ресурсам | 1Д: Вкл. (реком.)<br>1Г, 1В, 1Б: Вкл. (обяз.) | 2А: Вкл. (обяз.)<br>2Б: Вкл. (реком.) | Вкл. (реком.) |
| Журнал управления пользователями и группами | 1Д, 1Г: Вкл. (реком.)<br>1В, 1Б: Вкл. (обяз.) | Вкл. (реком.) | Вкл. (реком.) |
| Журнал печати | 1Д: Вкл. (реком.)<br>1Г, 1В, 1Б: Вкл. (обяз.) | 2А: Вкл. (обяз.)<br>2Б: Вкл. (реком.) | 3А: Вкл. (обяз.)<br>3Б: Вкл. (реком.) |
| Журнал управления политиками безопасности | 1Д, 1Г: Вкл. (реком.)<br>1В, 1Б: Вкл. (обяз.) | Вкл. (реком.) | Вкл. (реком.) |
| Системный журнал | Вкл. (реком.) | Вкл. (реком.) | Вкл. (реком.) |

**Таблица 3**

| Параметры | Класс защищенности | | |
|---|---|---|---|
| | 1Б, 1В, 1Г, 1Д | 2А, 2Б | 3А, 3Б |
| **Категория «Настройки пароля»** | **Значения параметров** | | |
| Минимальная длина пароля (0-14) | 1Б: не менее 8 симв. (обяз.)<br>1В, 1Г, 1Д: не менее 6 симв. (обяз.) | не менее 6 симв. (обяз.) | не менее 6 симв. (обяз.) |
| Наличие спецсимволов | 1Б: Да (реком.)<br>1В, 1Г, 1Д: Нет (АИБ) | Нет (АИБ) | Нет (АИБ) |
| Наличие цифр | Да (обяз.) | Да (обяз.) | Да (обяз.) |
| Наличие символов верхнего и нижнего регистра | 1Б: Да (реком.)<br>1В, 1Г, 1Д: Нет (АИБ) | Нет (АИБ) | Нет (АИБ) |
| Количество попыток неверного ввода пароля | 5 (реком.) | 5 (реком.) | 5 (реком.) |

Также необходимо настраивать параметры учетных записей следующим образом.

**Таблица 4**

| Параметры | Класс защищенности | | |
|---|---|---|---|
| | 1Б, 1В, 1Г, 1Д | 2А, 2Б | 3А, 3Б |
| Минимальный срок действия пароля | Нет (АИБ) | Нет (АИБ) | Нет (АИБ) |
| Максимальный срок действия пароля | Нет (АИБ) | Нет (АИБ) | Нет (АИБ) |
| Предупреждение о смене пароля | Нет (АИБ) | Нет (АИБ) | Нет (АИБ) |

**Таблица 5**

| Параметры | Класс защищенности | | |
|---|---|---|---|
| | 1Б, 1В, 1Г, 1Д | 2А, 2Б | 3А, 3Б |
| **Категория «Аппаратная целостность»** | **Значения параметров** | | |
| Проверять аппаратную целостность во время загрузки | Вкл. (обяз.) | Вкл. (обяз.) | Вкл. (обяз.) |
| Генерация событий аудита аппаратной целостности | Вкл. (реком.) | Вкл. (реком.) | Вкл. (реком.) |

**Таблица 6**

| Параметры | Класс защищенности | | |
|---|---|---|---|
| | 1Б, 1В, 1Г, 1Д | 2А, 2Б | 3А, 3Б |
| **Категория «Работа с доменом»** | **Значения параметров** | | |
| Домен | Нет (АИБ) | Нет (АИБ) | Нет (АИБ) |
| Разрешить авторизацию всем пользователям домена | Нет (АИБ) | Нет (АИБ) | Нет (АИБ) |

## 2. ГОСУДАРСТВЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

СЗИ НСД Dallas Lock Linux может быть использована в ГИС 1 класса защищенности. При определенных настройках СЗИ обеспечивает соответствие требованиям для 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.

Для соответствия классам защищенности ГИС должны быть настроены параметры безопасности, перечисленные в таблицах 7–12.

**Таблица 7**

| Параметры | Класс защищенности | | |
|---|---|---|---|
| | К1 | К2 | К3 |
| **Категория «Настройка сессий»** | **Значения параметров** | | |
| Максимальное количество сессий | не более 2 (обяз.) | 10 (реком.) | 10 (реком.) |
| Таймаут блокировки сессий (в минутах) | до 5 минут (обяз.) | до 15 минут (реком.) | 2 (АИБ) |

**Таблица 8**

| Параметры | Класс защищенности | | |
|---|---|---|---|
| | К1 | К2 | К3 |
| **Категория «Настройка аудита»** | **Значения параметров** | | |
| Срок хранения журналов. Установка срока хранения журналов (в месяцах) | не менее 3 (обяз.) | не менее 3 (обяз.) | не менее 3 (обяз.) |
| Журнал входов/выходов | Вкл. (обяз.) | Вкл. (обяз.) | Вкл. (обяз.) |
| Журнал доступа к ресурсам | Вкл. (обяз.) | Вкл. (обяз.) | Вкл. (обяз.) |
| Журнал управления пользователями и группами | Вкл. (обяз.) | Вкл. (обяз.) | Вкл. (реком.) |
| Журнал печати | Вкл. (обяз.) | Вкл. (обяз.) | Вкл. (реком.) |
| Журнал управления политиками безопасности | Вкл. (реком.) | Вкл. (реком.) | Вкл. (реком.) |
| Системный журнал | Вкл. (обяз.) | Вкл. (обяз.) | Вкл. (реком.) |

**Таблица 9**

| Параметры | Класс защищенности | | |
|---|---|---|---|
| | К1 | К2 | К3 |
| **Категория «Настройки пароля»** | **Значения параметров** | | |
| Минимальная длина пароля (0-14) | не менее 8 (обяз.) | не менее 6 (обяз.) | не менее 6 (обяз.) |
| Наличие спецсимволов | Да (обяз.) | Да (обяз.) | Да (обяз.) |
| Наличие цифр | Да (обяз.) | Да (обяз.) | Да (обяз.) |
| Наличие символов верхнего и нижнего регистра | Да (обяз.) | Да (обяз.) | Да (обяз.) |
| Количество попыток неверного ввода пароля | От 3 до 4 (обяз.) | От 3 до 8 (обяз.) | От 3 до 10 (обяз.) |

Также необходимо настраивать параметры учетных записей следующим образом:

**Таблица 10**

| Параметры | Класс защищенности | | |
|---|---|---|---|
| | К1 | К2 | К3 |
| Минимальный срок действия пароля | От 1 до 30 дней (обяз.) | От 1 до 30 дней (обяз.) | От 1 до 30 дней (обяз.) |
| Максимальный срок действия пароля | Не более 60 дней (обяз.) | Не более 90 дней (обяз.) | Не более 120 дней (обяз.) |
| Предупреждение о смене пароля | Нет (АИБ) | Нет (АИБ) | Нет (АИБ) |

**Таблица 11**

| Параметры | Класс защищенности | | |
|---|---|---|---|
| | К1 | К2 | К3 |
| **Категория «Аппаратная целостность»** | **Значения параметров** | | |
| Проверять аппаратную целостность во время загрузки | Да (обяз.) | Да (обяз.) | Да (реком.) |
| Генерация событий аудита аппаратной целостности | Да (обяз.) | Да (обяз.) | Да (реком.) |

**Таблица 12**

| Параметры | Класс защищенности | | |
|---|---|---|---|
| | К1 | К2 | К3 |
| **Категория «Работа с доменом»** | **Значения параметров** | | |
| Домен | Нет (АИБ) | Нет (АИБ) | Нет (АИБ) |
| Разрешить авторизацию всем пользователям домена | Нет (АИБ) | Нет (АИБ) | Нет (АИБ) |

## 3. ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

При определенных настройках СЗИ обеспечивает соответствие требованиям для ИСПДн, представленных в методическом документе «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 ИСПДн уровней защищенности 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».

Для соответствия уровням защищенности персональных данных должны быть настроены параметры безопасности, перечисленные в таблицах 13–18.

**Таблица 13**

| Параметры | Уровень защищенности ИСПДн | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| **Категория «Настройка сессий»** | **Значения параметров** | | | |
| Максимальное количество сессий | 10 (реком.) | 10 (реком.) | 10 (реком.) | 10 (реком.) |
| Таймаут блокировки сессий (в минутах) | 2 (АИБ) | 2 (АИБ) | 2 (АИБ) | 2 (АИБ) |

**Таблица 14**

| Параметры | Уровень защищенности ИСПДн | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| **Категория «Настройка аудита»** | **Значения параметров** | | | |
| Срок хранения журналов. Установка срока хранения журналов (в месяцах) | 3 (обяз.) | 3 (обяз.) | 3 (обяз.) | 3 (обяз.) |
| Журнал входов/выходов | Вкл. (обяз.) | Вкл. (обяз.) | Вкл. (обяз.) | Вкл. (обяз.) |
| Журнал доступа к ресурсам | Вкл. (обяз.) | Вкл. (обяз.) | Вкл. (обяз.) | Вкл. (обяз.) |

Продолжение **Таблицы 14**

| Параметры | Уровень защищенности ИСПДн | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| Журнал управления пользователями и группами | Вкл. (обяз.) | Вкл. (обяз.) | Вкл. (реком.) | Вкл. (реком.) |
| Журнал печати | Вкл. (АИБ) | Вкл. (АИБ) | Вкл. (АИБ) | Вкл. (АИБ) |
| Журнал управления политиками безопасности | Вкл. (обяз.) | Вкл. (обяз.) | Вкл. (реком.) | Вкл. (реком.) |
| Системный журнал | Вкл. (обяз.) | Вкл. (обяз.) | Вкл. (обяз.) | Вкл. (обяз.) |

**Таблица 15**

| Параметры | Уровень защищенности ИСПДн | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| **Категория «Настройки пароля»** | **Значения параметров** | | | |
| Минимальная длина пароля (0-14) | 8 симв. (обяз.) | 6 симв. (обяз.) | 6 симв. (обяз.) | 6 симв. (обяз.) |
| Наличие спецсимволов | Да (обяз.) | Да (обяз.) | Да (обяз.) | Да (обяз.) |
| Наличие цифр | Да (обяз.) | Да (обяз.) | Да (обяз.) | Да (обяз.) |
| Наличие символов верхнего и нижнего регистра | Да (обяз.) | Да (обяз.) | Да (обяз.) | Да (обяз.) |
| Количество попыток неверного ввода пароля | От 3 до 4 (обяз.) | От 3 до 8 (обяз.) | От 3 до 10 (обяз.) | От 3 до 10 (обяз.) |

Также необходимо настраивать параметры учетных записей следующим образом:

**Таблица 16**

| Параметры | Уровень защищенности ИСПДн | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| 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.) |
| Максимальный срок действия пароля | Не более 60 дней (обяз.) | Не более 90 дней (обяз.) | Не более 120 дней (обяз.) | Не более 180 дней (обяз.) |
| Предупреждение о смене пароля | Нет (АИБ) | Нет (АИБ) | Нет (АИБ) | Нет (АИБ) |

**Таблица 17**

| Параметры | Уровень защищенности ИСПДн | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| **Категория «Аппаратная целостность»** | **Значения параметров** | | | |
| Проверять аппаратную целостность во время загрузки | Вкл. (обяз.) | Вкл. (обяз.) | Вкл. (реком.) | Вкл. (реком.) |
| Генерация событий аудита аппаратной целостности | Вкл. (реком.) | Вкл. (реком.) | Вкл. (реком.) | Вкл. (реком.) |

**Таблица 18**

| Параметры | Уровень защищенности ИСПДн | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| **Категория «Работа с доменом»** | **Значения параметров** | | | |
| Домен | Нет (АИБ) | Нет (АИБ) | Нет (АИБ) | Нет (АИБ) |
| Разрешить авторизацию всем пользователям домена | Нет (АИБ) | Нет (АИБ) | Нет (АИБ) | Нет (АИБ) |

Продолжение **Таблицы №4**

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:**