Лабораторная работа №5

НАТСРОЙКА ДОВЕРЕННОЙ ЗАГРУЗКИ ПРИ ПОМОЩИ СЗИ DALLAS LOCK

1. **Цели и задачи работы**

Получение навыков организации доверенной загрузки при помощи СЗИ от НСД Dallas Lock

2**. Теоретические положения**

Одним из важных элементов системы защиты от несанкционированного доступа к ресурсам автоматизированной вычислительной системы является использование модуля доверенной загрузки.

Под доверенной загрузкой обычно понимается загрузка операционной системы с внутреннего жесткого диска компьютера, которая происходит только после выполнения процедур идентификации и аутентификации пользователя, а также проверки целостности программной и аппаратной среды рабочего места, в том числе целостности объектов загружаемой ОС.

На сегодняшний день большинство средств доверенной загрузки реализуются на двух основных способах:

– с использованием аппаратного контроллера, который устанавливается в ПК и выполняет функции по организации доверенной загрузки системы;

– изменение главной загрузочной записи жесткого диска.

К первому классу относятся такие программно-аппаратные средства защиты информации, как ПАК «Соболь», «Аккорд_АМДЗ», «КРИПТОН-ЗАМОК». Данные средства обеспечивают высокий уровень защищенности, так как обеспечивают выполнение основных задач по защите до загрузки системы. При этом злоумышленнику сложно модифицировать данные СЗИ вследствие ограниченности информации о их реализации. Недостатками данных решений является относительно высокая цена и ориентированность на персональные компьютеры: поддерживаемые ими интерфейсы практически не позволяют их использовать на

ноутбуках.

СЗИ второго класса начинают работать после выполнения BIOS и передачи управления программе в главной загрузочной записи жесткого диска. Обычно в MBR записывается собственная программа средства защиты, которая осуществляет идентификацию и аутентификацию пользователя, проверку целостности программно-аппаратных средств компьютера. Примерами подобных систем являются «Страж NT», «Dallas Lock».

Для успешного использования модулей обеспечения доверенной загрузки операционной системы необходимо использовать физические средства защиты, ограничивающие доступ злоумышленника к системному блоку.

Дополнительным элементом защиты модуля доверенной загрузки Dallas Lock является прозрачное шифрование информации, хранящейся на локальных, а также съемных жестких дисках.

3. **Системные требования**

1. Компьютер IBM PC, x86 или x63.
2. Процессор не менее Pentium D с частотой не менее 1.7 ГГц.
3. Не менее 2 ГБ ОЗУ
4. Не менее 20 Гб ПЗУ.
5. ОС Windows 7, или более новая разрядностью 32 или 64 бита.
6. Наличие USB порта версии не менее 2.0
7. Наличие открытого порта 80.
8. Поддержка протокола TCP/IP.
9. Наличие установленной СЗИ Dallas Lock 8.0, или комплекта ПО, позволяющего произвести установку СЗИ Dallas Lock 8.0 на выбранный ПК.

4. **Постановка задачи**

1. Активировать модуль доверенной загрузки операционной системы;

2. Создать зону на жестком диске, предназначенную для прозрачного криптографического преобразования.

3. Проверку корректности работы системы доверенной загрузки, реализованной на основе СЗИ НСД DALLAS LOCK, а так же корректность работы системы криптографического преобразования зон жёстких дисков, встроенных в СЗИ НСД DALLAS LOCK.

5. **Порядок выполнения работы**

1.Зайдите в систему с правами администратора. Запустите программу администрирования Dallas Lock и перейдите на вкладку «Параметры безопасности». Да- лее выберите категорию «Доверенная загрузка».

2.В области «Действия» нажмите на кнопку «Включить». В появившемся диалоговом окне введите PIN-код администратора и алгоритм преобразования диска, как показано на рисунке 3.1.

3.Подождите пока завершится процесс активации доверенной загрузки и нажмите кнопку «OK» в окне с сообщением о необходимости перезагрузки системы.

4.Для создания PIN-кода пользователя нажмите в области действии на кнопку «PIN-коды». Обратите внимание, что если на панели инструментов не хватает места для всех значков, то они сворачиваются. Например, на рисунке 3.2 представлен вариант, когда список действий в пункте меню «Доверенная загрузка» свёрнуты.

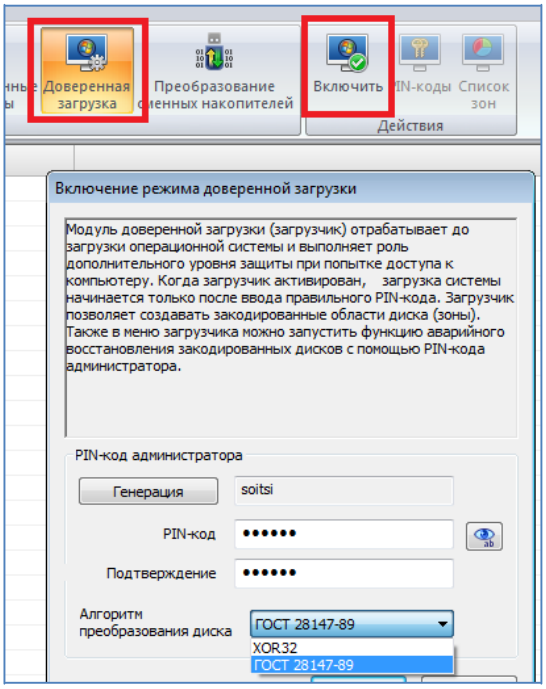

Рисунок 3.1 –Включение режима доверенной загрузки

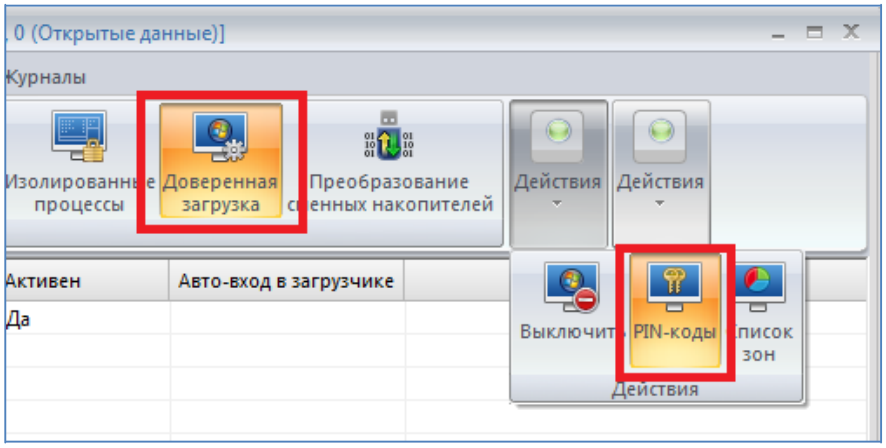

Рисунок 3.2 – Выбор действия «PIN-коды»

5.Нажмите на панели действий кнопку «Добавить PIN», как на рисунке 3.3

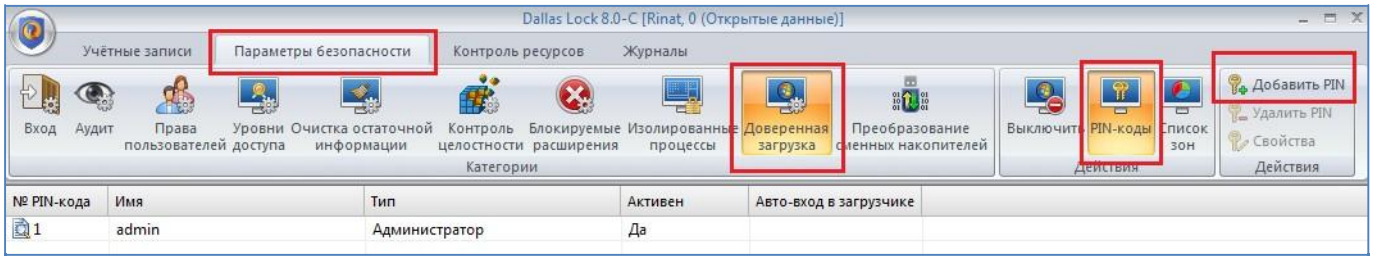

Рисунок 3.3 –Выбор действия «Добавить PIN»

6.В появившемся диалоговом окне введите произвольное имя PIN-кода, например, user1. Далее введите новый PIN-код, который будет использоваться при идентификации при загрузке системы. Пример заполнения полей данного действия представлен на рисунке 3.3.

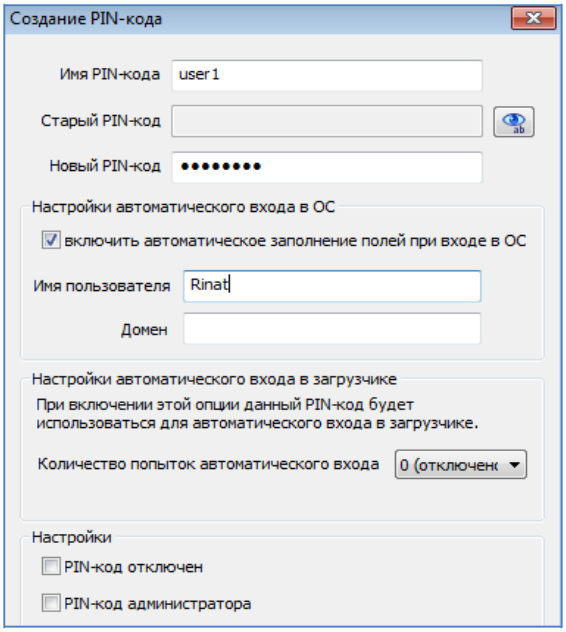

Рисунок 3.4 – Окно создания PIN-кода для загрузчика

7.Закройте программу администрирования Dallas Lock 8.0 и перезагрузите компьютер.

8.В окне авторизации введите PIN-код для загрузки системы (рисунок 3.5). При активном загрузчике Dallas Lock 8.0-C в момент загрузки компьютера к нему не должны быть подключены загрузочные USB-flash-диски.

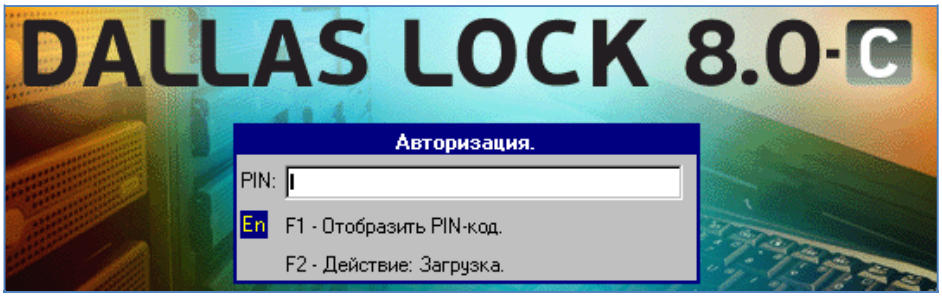

Рисунок 3.5 – Окно авторизации загрузки

9.Зайдите в систему учетной записью с правами администратора СЗИ Dallas Lock. Запустите программу администрирования Dallas Lock и перейдите на вкладку
«Параметры безопасности».

10. Перейдите на вкладку «Список зон» и нажмите на кнопку действия «Добавить зону», как показано на рисунке 3.6. В данной работе выберите область преобразования «Системная область» (преобразование всего диска может потребовать много времени).

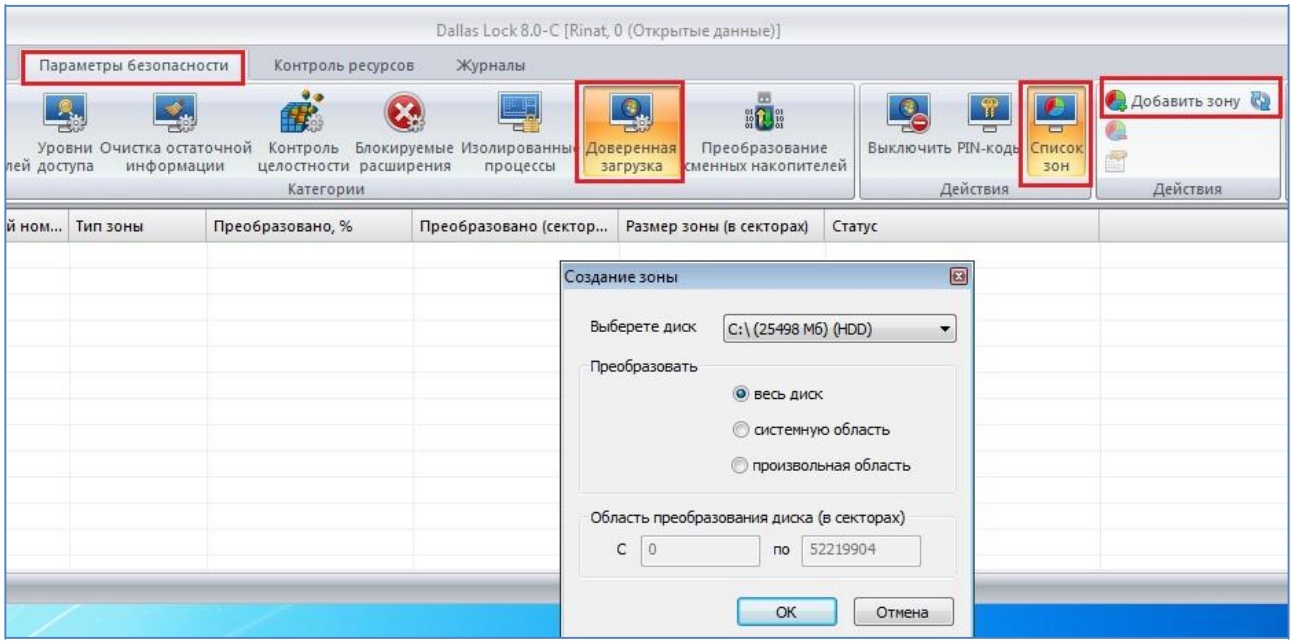

Рисунок 3.6 – Параметры создания зоны преобразования

11. Ответить на контрольные вопросы и составить отчет по работе.

Контрольные вопросы

1. Дайте определение понятия доверенной загрузки.
2. Как реализован механизм доверенной загрузки в СЗИ Dallas Lock?
3. Как реализован механизм доверенной загрузки в ПАК «Соболь», «Ак- корд_АМДЗ», «КРИПТОН-ЗАМОК?
4. Опишите механизм прозрачного преобразования дисков, реализованный в Dallas Lock.