



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Колледж программирования и кибербезопасности

Отчет о выполнении практического задания
по дисциплине «МДК.01.04 Эксплуатация автоматизированных
(информационных) систем в защищенном исполнении»

Практическое задание № 16

Специальность – 10.05.02 Информационная безопасность
телекоммуникационных систем

Выполнил студент:

_____ Маркаров М. О.

Группа: ИБ-32

Руководитель:

_____ Герасин В. Ю.

Работа защищена с оценкой _____

Дата защиты _____

Москва

2025

Практическая работа № 16

Тема: централизованное управление системой защиты, оперативный мониторинг и аудит безопасности.

Цель: приобретение необходимого объёма знаний и практических навыков в области централизованного управления системой защиты, оперативного мониторинга и аудита безопасности.

Ход работы:

Задание 1. На виртуально машине с СЗИ Dallas Lock 8.0 просмотреть журнал событий НСД.

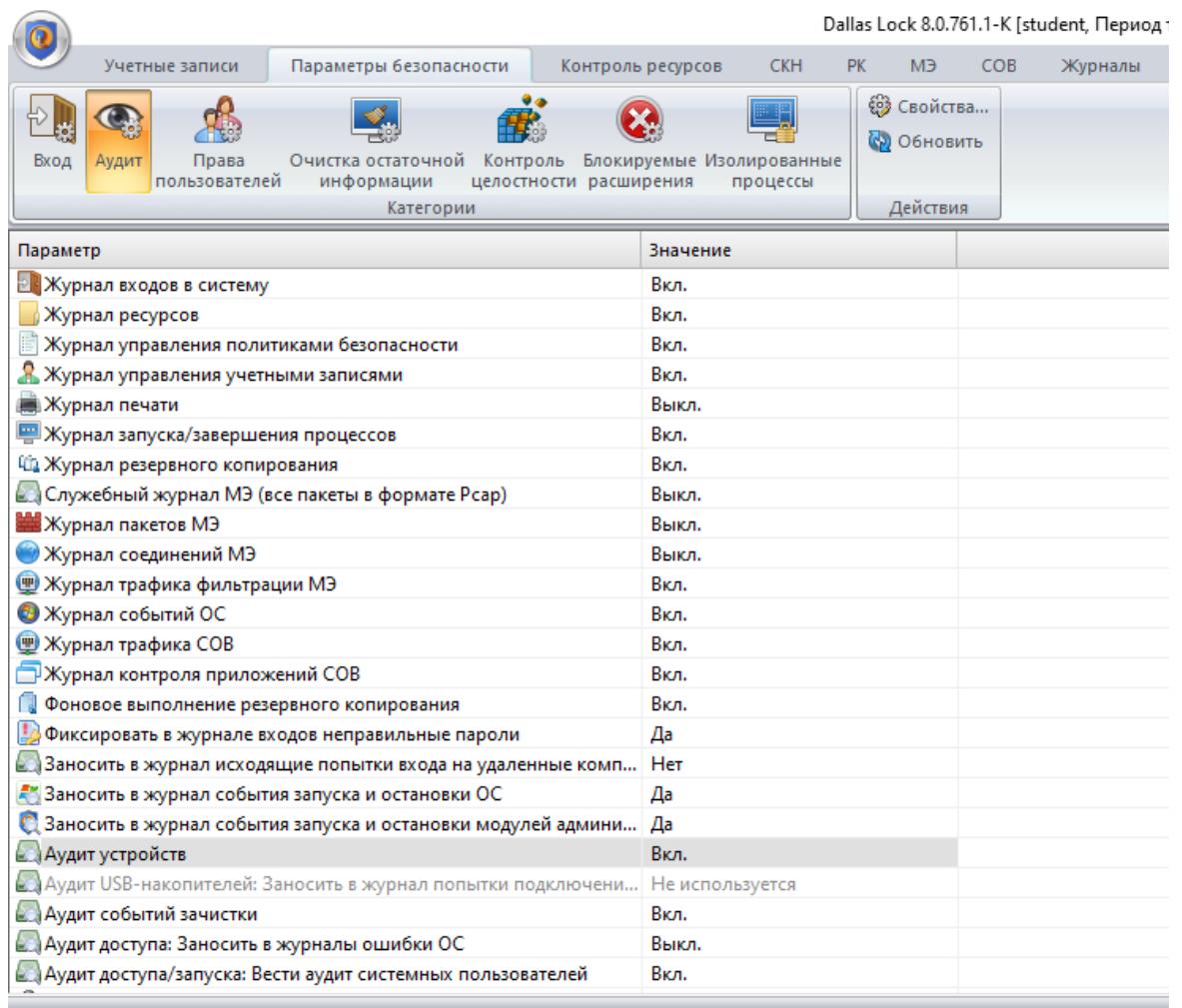


Рис. 1 настройка пользователей используя Аудит

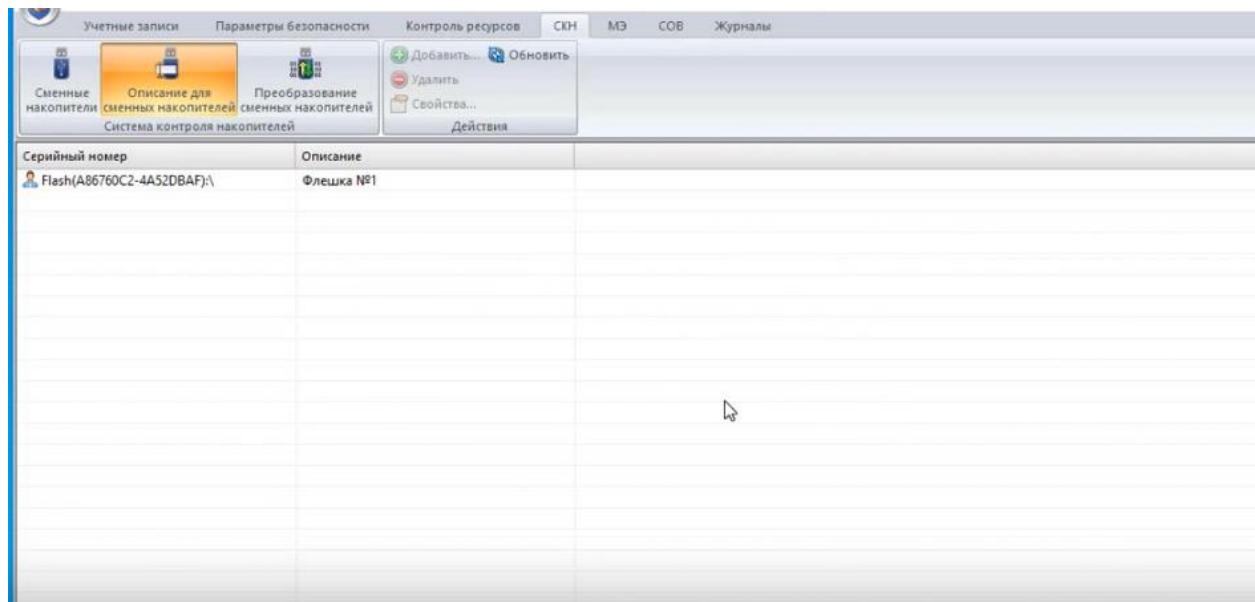


Рис. 2 Пользователь с защитой с входом по флешке

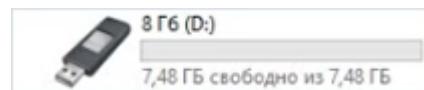


Рис. 3 Результат проделанной работы

Задание 2. На виртуально машине с СЗИ Secret Net Studio8.9 просмотреть журнал событий НСД.

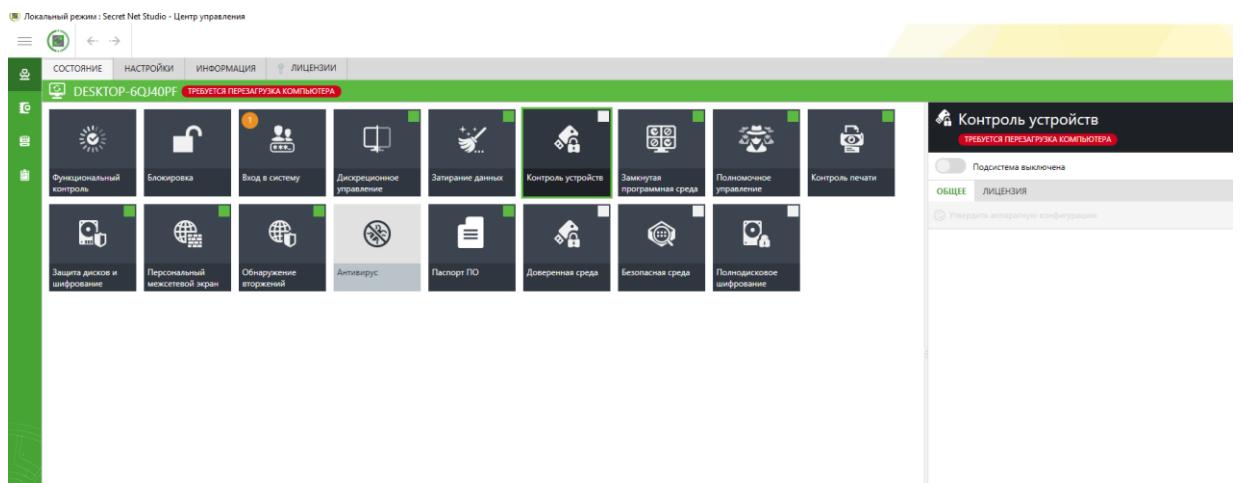


Рис. 4 Основной экран Secret net studio

Рис. 5 Результат сканирования

Рис. 6 Результат сканирования безопасности

СОБЫТИЯ		УГРОЗЫ						
	Дата	Журнал	Событие	Категория	Источник	Компьютер	Домен	Пользователь
ЖУРНАЛЫ								
Secret Net Studio	26.03.2025...	Системный	10016		Microsoft...	DESKTOP-6QJ...	DESKTOP-6...	student
Безопасности	26.03.2025...	Системный	10016		Microsoft...	DESKTOP-6QJ...	DESKTOP-6...	student
Системный	26.03.2025...	Системный	10016		Microsoft...	DESKTOP-6QJ...	NT AUTHO...	СИСТЕМА
Приложений	26.03.2025...	Системный	10016		Microsoft...	DESKTOP-6QJ...	NT AUTHO...	СИСТЕМА
Все тревоги	26.03.2025...	Системный	10016		Microsoft...	DESKTOP-6QJ...	DESKTOP-6...	student
Тревоги повышенного уровня	26.03.2025...	Системный	7040		Service Con...	DESKTOP-6QJ...	NT AUTHO...	СИСТЕМА
ВНЕШНИЕ ЖУРНАЛЫ								
	26.03.2025...	Системный	7040		Service Con...	DESKTOP-6QJ...	NT AUTHO...	СИСТЕМА
	26.03.2025...	Системный	10016		Microsoft...	DESKTOP-6QJ...	NT AUTHO...	NETWORK SE
	26.03.2025...	Системный	10016		Microsoft...	DESKTOP-6QJ...	NT AUTHO...	NETWORK SE
	26.03.2025...	Системный	7001	(1101)	Microsoft...	DESKTOP-6QJ...	NT AUTHO...	СИСТЕМА
	26.03.2025...	Системный	7026		Service Con...	DESKTOP-6QJ...	NT AUTHO...	СИСТЕМА
	26.03.2025...	Системный	7000		Service Con...	DESKTOP-6QJ...	NT AUTHO...	LOCAL SER
	26.03.2025...	Системный	51046	События со...	Microsoft...	DESKTOP-6QJ...	NT AUTHO...	LOCAL SER
	26.03.2025...	Системный	50103	События со...	Microsoft...	DESKTOP-6QJ...	NT AUTHO...	LOCAL SER
	26.03.2025...	Системный	50036	События со...	Microsoft...	DESKTOP-6QJ...	NT AUTHO...	LOCAL SER
	26.03.2025...	Системный	6		Microsoft...	DESKTOP-6QJ...	NT AUTHO...	СИСТЕМА
	26.03.2025...	Системный	6		Microsoft...	DESKTOP-6QJ...	NT AUTHO...	СИСТЕМА
	26.03.2025...	Системный	6		Microsoft...	DESKTOP-6QJ...	NT AUTHO...	СИСТЕМА
	26.03.2025...	Системный	1		Microsoft...	DESKTOP-6QJ...	NT AUTHO...	СИСТЕМА
	26.03.2025...	Системный	6		Microsoft...	DESKTOP-6QJ...	NT AUTHO...	СИСТЕМА
	26.03.2025...	Системный	6		Microsoft...	DESKTOP-6QJ...	NT AUTHO...	СИСТЕМА
	26.03.2025...	Системный	6		Microsoft...	DESKTOP-6QJ...	NT AUTHO...	СИСТЕМА

Рис. 7 Результат сканирования системы

СОБЫТИЯ		УГРОЗЫ							
	Дата	Журнал	Событие	Категория	Источник	Компьютер	Домен	Пользователь	Создано
СОБЫТИЯ									
SECRET NET STUDIO	26.03.2025...	Приложений	16384	Общие	Microsoft-...	DESKTOP-6QJ...			
Безопасности	26.03.2025...	Приложений	327	Общие	ESENT	DESKTOP-6QJ...			
Системный	26.03.2025...	Приложений	326	Общие	ESENT	DESKTOP-6QJ...			
Приложений	26.03.2025...	Приложений	327	Общие	ESENT	DESKTOP-6QJ...			
Все тревоги	26.03.2025...	Приложений	326	Общие	ESENT	DESKTOP-6QJ...			
Тревоги повышенного уровня	26.03.2025...	Приложений	327	Общие	ESENT	DESKTOP-6QJ...			
НЕШИЕ ЖУРНАЛЫ									
	26.03.2025...	Приложений	326	Общие	ESENT	DESKTOP-6QJ...			
	26.03.2025...	Приложений	327	Общие	ESENT	DESKTOP-6QJ...			
	26.03.2025...	Приложений	326	Общие	ESENT	DESKTOP-6QJ...			
	26.03.2025...	Приложений	15		SecurityCen...	DESKTOP-6QJ...			
	26.03.2025...	Приложений	327	Общие	ESENT	DESKTOP-6QJ...			
	26.03.2025...	Приложений	326	Общие	ESENT	DESKTOP-6QJ...			
	26.03.2025...	Приложений	327	Общие	ESENT	DESKTOP-6QJ...			
	26.03.2025...	Приложений	326	Общие	ESENT	DESKTOP-6QJ...			
	26.03.2025...	Приложений	327	Общие	ESENT	DESKTOP-6QJ...			
	26.03.2025...	Приложений	326	Общие	ESENT	DESKTOP-6QJ...			
	26.03.2025...	Приложений	1		SecurityCen...	DESKTOP-6QJ...			
	26.03.2025...	Приложений	16394		Microsoft-...	DESKTOP-6QJ...			
	26.03.2025...	Приложений	900		Microsoft-...	DESKTOP-6QJ...			
	26.03.2025...	Приложений	0		edgeupdate	DESKTOP-6QJ...			
	26.03.2025...	Приложений	326	Общие	ESENT	DESKTOP-6QJ...			
	26.03.2025...	Приложений	105	Общие	ESENT	DESKTOP-6QJ...			

Рис. 8 Результат сканирования приложений

Задание 3. Провести сравнение журналов Dallas Lock 8.0 и Secret Net Studio 8.9. Выделить основные преимущества и недостатки журналов СЗИ.

Dallas Lock 8.0-C [superadm; 0 (Открытые данные)]

Учетные записи		Контроль доступа		Параметры безопасности		Журналы					
Журнал входов		Журнал управл. уч/записями		Журнал доступа к ресурсам		Журнал печати		Журнал политиками		Журнал процессов из файла	
Категории											
Время		Пользователь		Имя		Результат		Операция			
	24.01.2013 10:46:04	superadm	user855645212	OK						Создать пользователя	
	24.01.2013 10:44:56	superadm	alexandr	OK						Создать пользователя	
	24.01.2013 10:44:50	superadm	vlad	OK						Создать пользователя	
	24.01.2013 10:41:29	LOCAL_SYSTEM	stud	Пользователь ук...						Запросить параметры пользователя	
	24.01.2013 10:41:29	LOCAL_SYSTEM	test	Пользователь ук...						Запросить параметры пользователя	
	24.01.2013 10:40:46	superadm	user517210898	OK						Удалить пользователя	
	24.01.2013 10:40:30	superadm	user517210898	OK						Создать пользователя	
	24.01.2013 10:35:14	LOCAL_SYSTEM	"\\"	OK						Создать пользователя	
	25.12.2012 14:28:00	superadm	superadm	OK						Сменить пароль пользователя	
	25.12.2012 13:02:59	superadm	superadm	OK						Сменить пароль пользователя	

Рис. 9 Dallas Lock 8.0

Приемущества

Интеграция с другими системами: Возможность интеграции с различными корпоративными системами и приложениями.

Поддержка различных платформ: Работает на различных операционных системах, что делает его более универсальным.

Недостатки программы

Сложности с обновлениями: Обновления могут быть не всегда интуитивно понятны, что затрудняет процесс их установки.

Проблемы с поддержкой: Некоторые пользователи сообщают о затруднениях в получении технической поддержки.

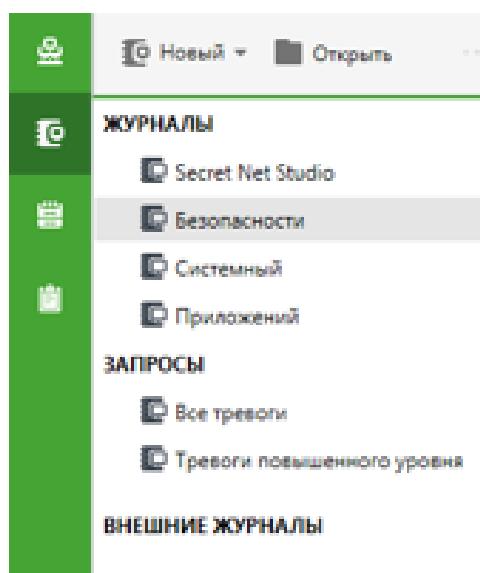


Рис. 10 Secret Net Studio 8.9 главное меню журнала

Приемущества

Высокий уровень безопасности: Использует современные криптографические алгоритмы и методы защиты, что обеспечивает высокий уровень безопасности данных.

Гибкость настройки: Позволяет пользователям настраивать параметры безопасности под свои нужды, что делает систему более адаптивной.

Поддержка многоуровневой аутентификации: Включает многофакторную аутентификацию, что повышает уровень защиты.

Недостатки:

Сложный интерфейс: Некоторые пользователи могут столкнуться с трудностями в освоении интерфейса, который может показаться перегруженным.

Вывод: на основе документации мы смогли провести ряд задач и извлекли из этого, создав таким образом отчёт подчёркивающий актуальность программ.