Лабораторная работа №2 "Настройка политик безопасности для Secret Net Studio 8.5"

ХОД РАБОТЫ

1. Загрузите ОС Windows под учетной записью администратора.

2. Откройте "Локальный центр управления" ("Пуск → Все программы → Код Безопасности → Secret Net Studio → Локальный центр управления") (Рис. 1).

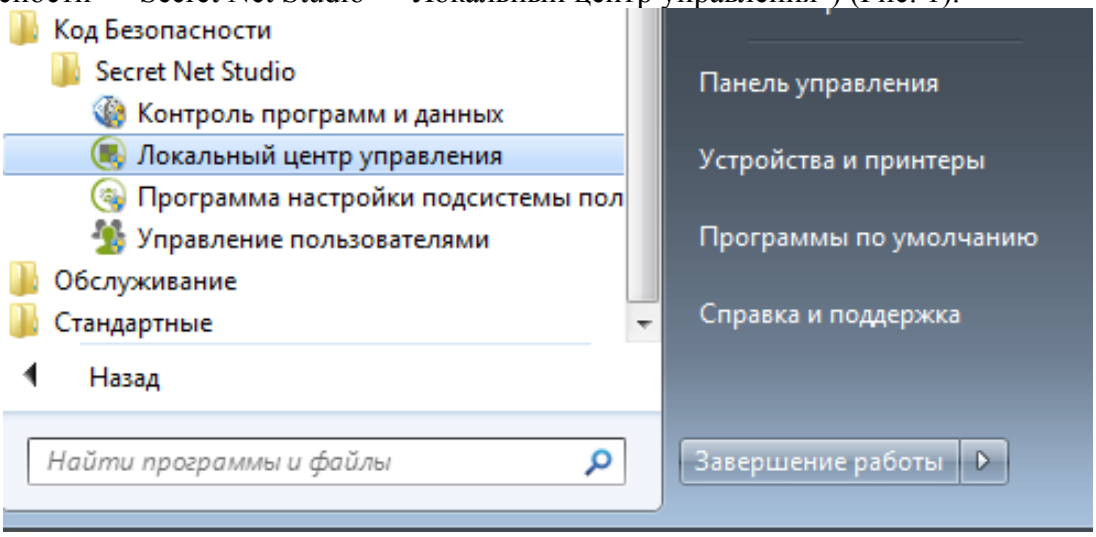

Рис. 1. Раздел «Код безопасности» в меню «Пуск».

3. После запуска окна приложения выберите вкладку «НАСТРОЙКИ» (Рис. 2, обозначено цифрой 1).

4. Выберите интересующею группу из раздела «ПОЛИТИКИ» в левой части окна приложения (Рис. 2, обозначено цифрой 2). Политики безопасности в Secret Net Studio 8.5 разделены на базовые группы:

1) **базовая защита** ("Вход в систему", "Журнал", "Теневое копирование", "Ключи пользователя", "Оповещение о тревогах", "Контроль RDP подключений", "Администрирование системы защиты") — объединяет параметры функционирования механизмов базовой защиты клиента;

2) **локальная защита** ("Дискреционное управление доступом", "Затирание данных", "Полномочное управление доступом", "Замкнутая программная среда", "Защита диска и шифрование данных") — объединяет параметры функционирования механизмов локальной защиты клиента;

3) **сетевая защита** ("Персональный межсетевой экран") — объединяет параметры функционирования механизмов сетевой защиты клиента;

4) **контроль устройств** — содержит параметры функционирования механизмов контроля подключения и изменения устройств и разграничения доступа к устройствам;

5) **контроль печати** — содержит параметры для настройки маркировки документов, теневого копирования, списка используемых принтеров и политик прямой печати;

6) **антивирус** — содержит параметры для настройки постоянной защиты, режимов сканирования, списка исключений и сканирования по расписанию;

7) **обнаружение вторжения** — содержит параметры для настройки детекторов сетевых атак и сигнатурных анализаторов;

8) **обновление** — содержит параметры автоматической проверки обновлений антивирусных баз и базы правил;

9) **паспорт ПО** — содержит параметры настройки сбора данных о состоянии программной среды (СПС) по расписанию, выбранных каталогов и расширения файлов.

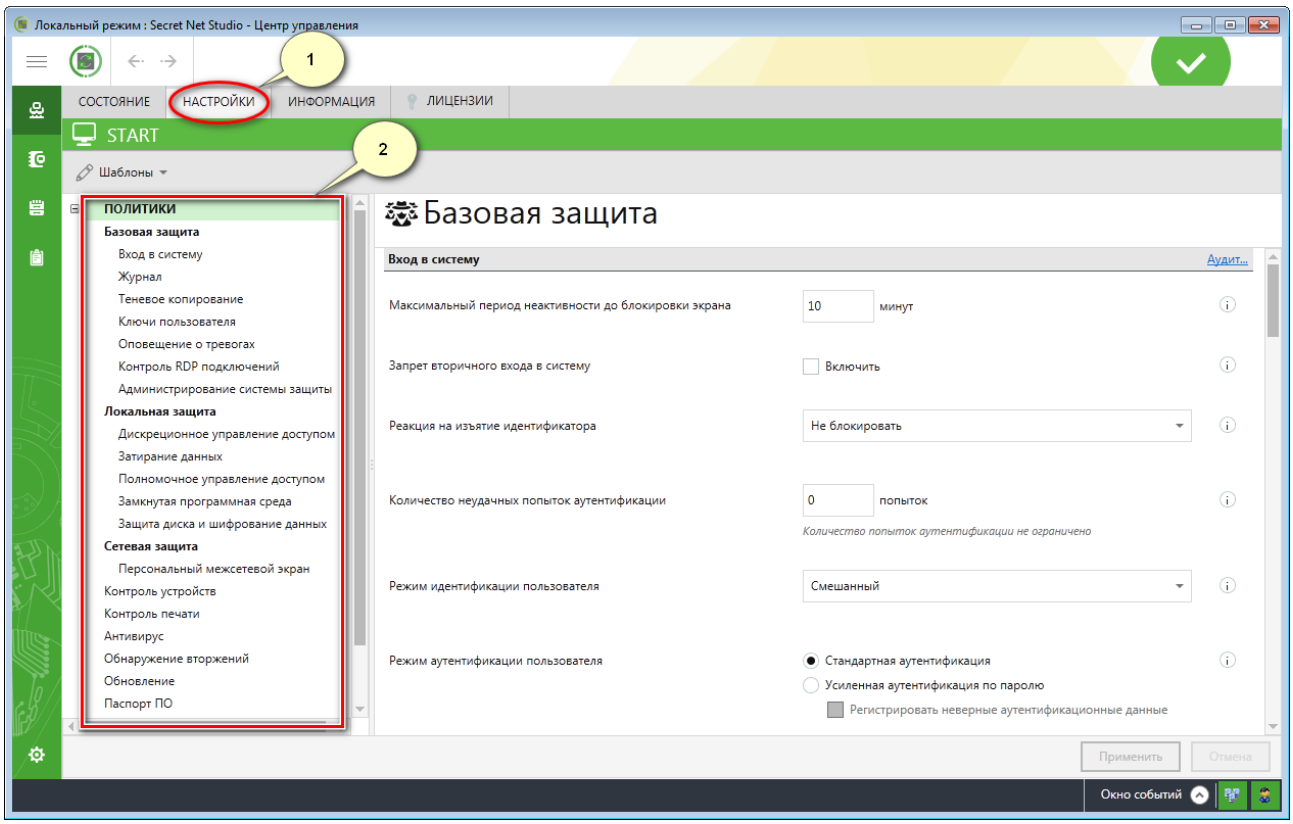

Рис. 2. Вкладка «Настройки» окна «Центра управления».

5. В центральной части окна приложения находятся параметры безопасности (Рис. 3). Перейдите группу «Базовая защита» и выполните настройки в соответствии с заданием.

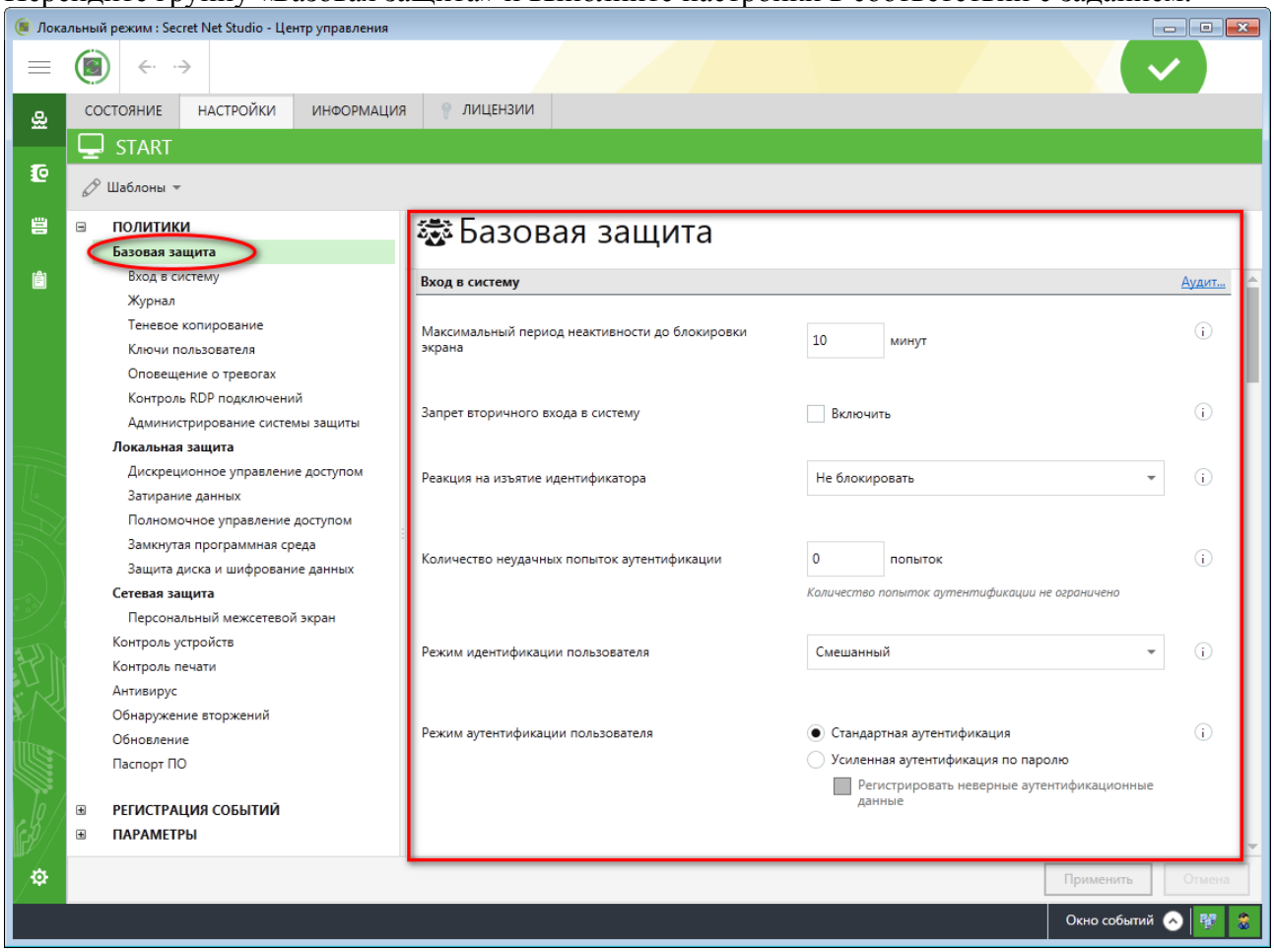

Рис. 3. Вкладка «Настройки» группа «Базовая защита».

Если нажать левой кнопкой мыши на знак «i», который располагается рядом с параметром, можно увидеть описания параметра (Рис. 4).

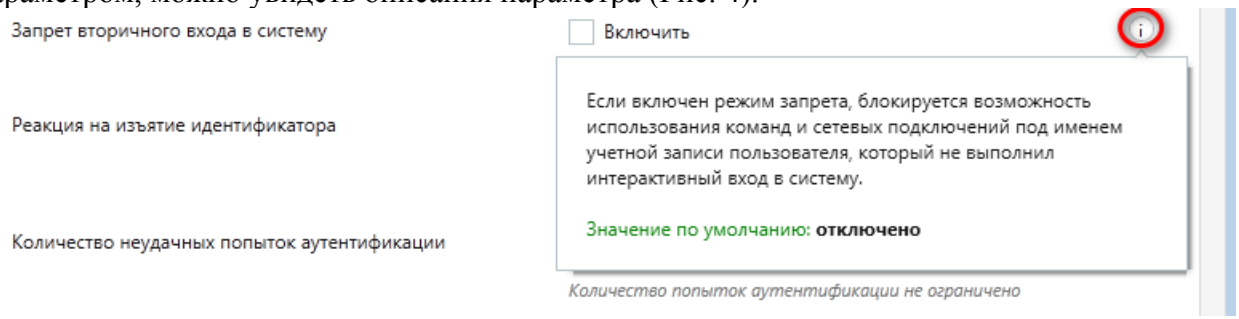

Рис. 4. Кнопка информация («i») в окне приложения.

6. После настройки выбранных параметров нажмите кнопку «Переменить» в правом нижнем углу окна приложения (Рис. 5).

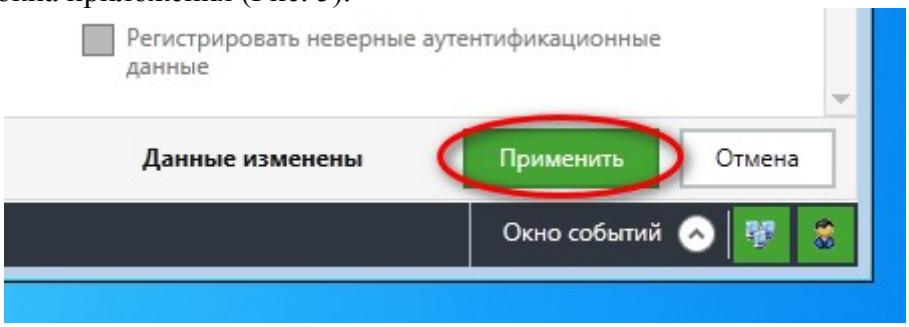

Рис. 5. Расположение кнопки «Применить» в окне приложения.

ЗАДАНИЕ

№ п/п	Параметр настройки	Задаваемое значение
1	Максимальный период не активности до блокировки экрана	15 минут
2	Запрет вторичного входа в систему	Включено
3	Режим идентификации пользователя	По имени
4	Количество неудачных попыток аутентификации	12 попыток
5	Максимальный размер журнала системы защиты	4096 КБ
6	Политика перезаписи событий	Затирать события по мере необходимости
7	Режим аутентификации пользователя	Стандартная аутентификация
8	Оповещение пользователя	Оповещать пользователя о последнем успешном входе в систему
9	Теневое копирование: Размер хранилища	15%
10	Перенаправление устройств в RDP-подключениях: Устройств Plug and Play	Запрещено подключать удаленные устройства к компьютеру
11	Перенаправление принтеров в RDP-подключениях	Запрещено использование принтеры компьютера удаленно
12	Самозащита продукта	Включить