



Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

Институт кибербезопасности и цифровых технологий
Кафедра КБ-1 «Защита информации»

ОТЧЕТ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКОЙ РАБОТЫ №2

Дисциплина: «Разработка и эксплуатация защищенных
автоматизированных систем»

Тема: «Защита данных рабочего места пользователя
автоматизированной системы SNS»

Выполнил:

Студент группы БАСО-03-20

Усков К.А.

Проверил:

доцент Федин Ф.О.

Москва, 2024

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	3
1 ЗАДАНИЕ №1	4
2 ЗАДАНИЕ №2	9
3 ЗАДАНИЕ №3	12
4 ЗАДАНИЕ №4	21
5 ЗАДАНИЕ №5	24
6 ЗАДАНИЕ №6	27
7 ЗАДАНИЕ №7	34
8 ЗАДАНИЕ №8	40
9 ЗАДАНИЕ №9	45
ВЫВОД	49

ВВЕДЕНИЕ

Учебная цель занятия:

1. Углубить теоретические знания и выработать практические умения в области защиты информации автоматизированных систем с использованием SNS.
2. Сформировать у студентов научное мировоззрение, высокие морально-психологические качества, привить любовь к своей профессии, стремление к повышению своего профессионального мастерства, творческий подход к выполнению поставленных задач, умение работать в коллективе, правильно оценивать результаты своего труда.

Место проведения занятия: компьютерная аудитория.

Учебно-материальное обеспечение:

- 1) Учебный компьютерный класс с ПЭВМ (лаборатория).
- 2) Secret Net Studio 8.5 (или 8.6).

1 ЗАДАНИЕ №1

Установка автономного варианта SNS на рабочем месте пользователя автоматизированной системы в защищенном исполнении.

Ход выполнения задания

С официального сайта компании «Код безопасности», из центра загрузок (рисунок 1.1) были скачены файлы для установки демоверсии SNS 8.11 - https://www.securitycode.ru/download_center/?section=downloads&product=Secret%20Net%20Studio&version=8.11

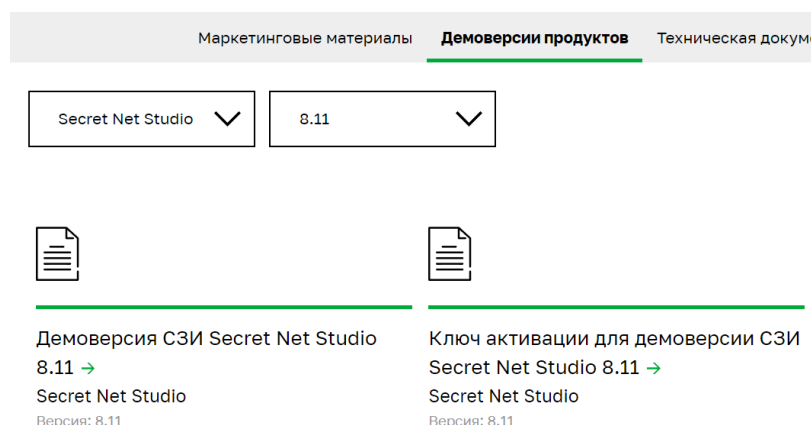


Рисунок 1.1

После скачивания был запущен исполняемый файл из папки с демоверсией, рисунок 1.2.

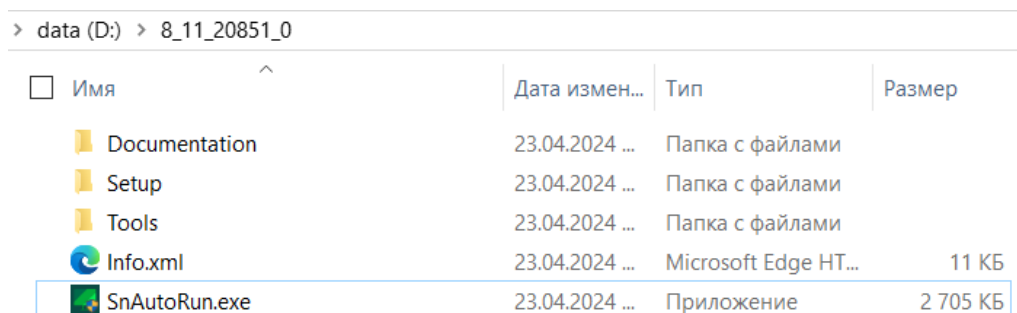


Рисунок 1.2

В открывшемся диалоговом окне был выбран пункт «Защитные компоненты» для начала процесса установки, рисунок 1.3.

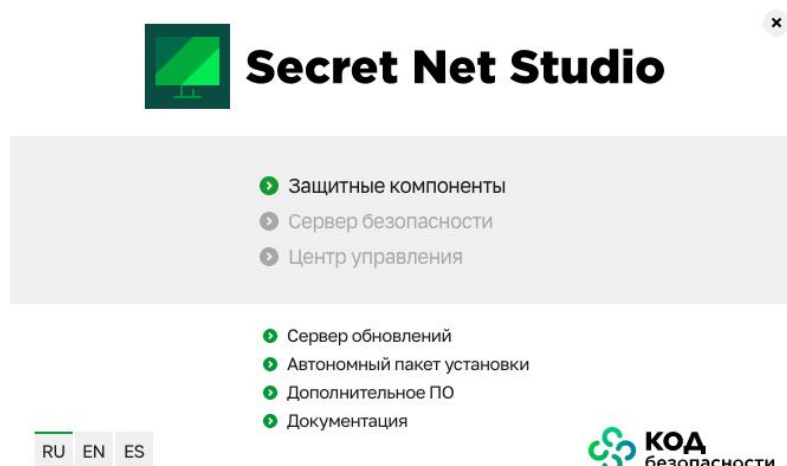


Рисунок 1.3

Было внимательно изучено и принято лицензионное соглашение, рисунок 1.4.

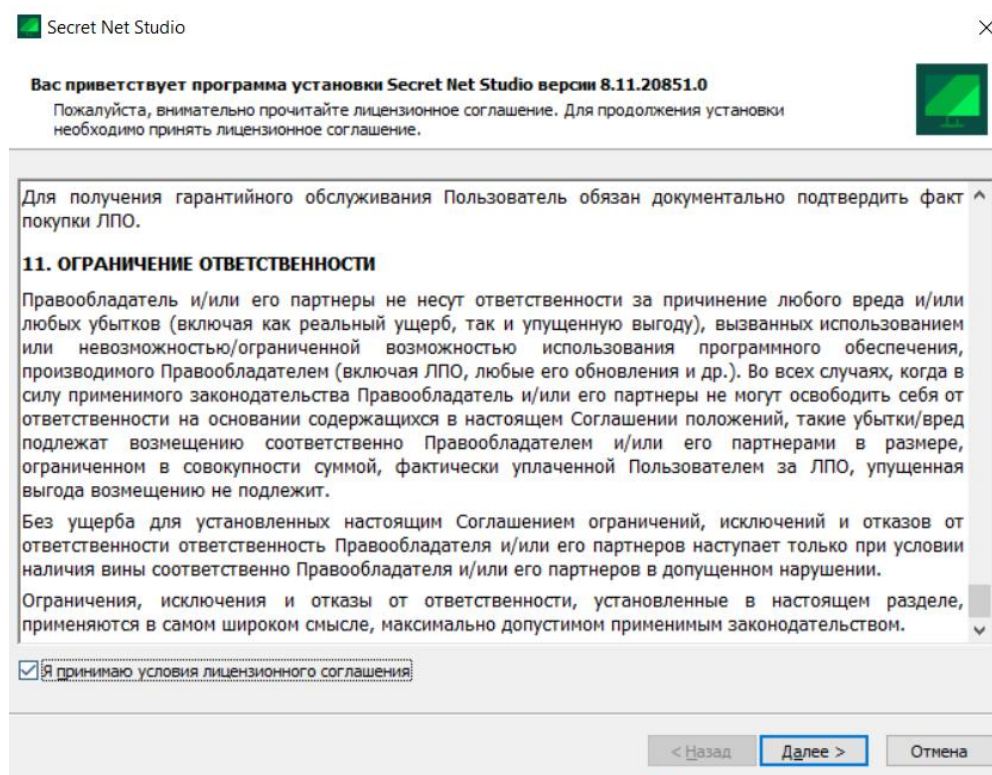


Рисунок 1.4

В качестве режима установки был выбран автономный, рисунок 1.5.



Рисунок 1.5

Компоненты защиты были выбраны с помощью скаченного файла лицензии, рисунок 1.6.

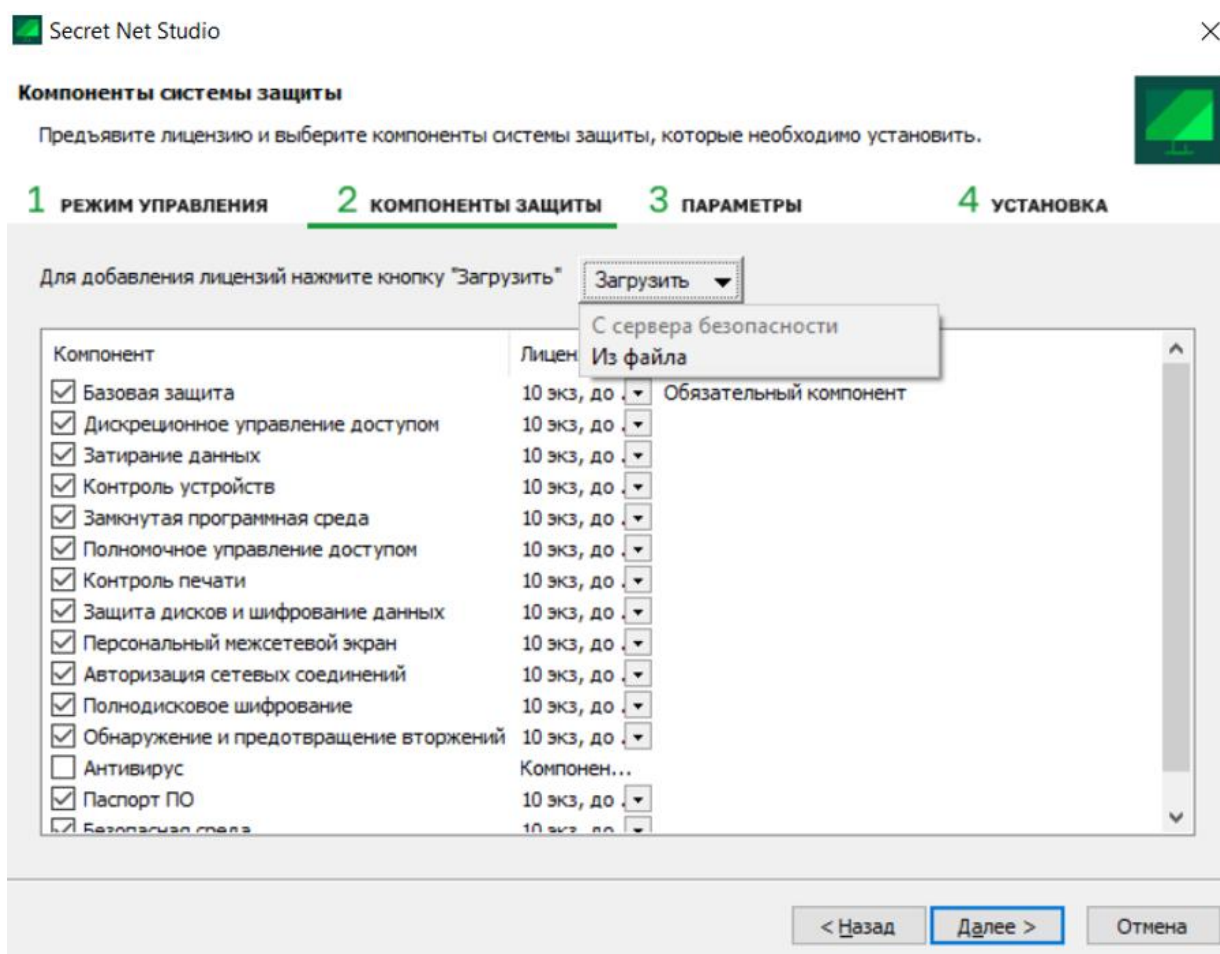


Рисунок 1.6

Затем было выбрано место для загрузки программы, рисунок 1.7.

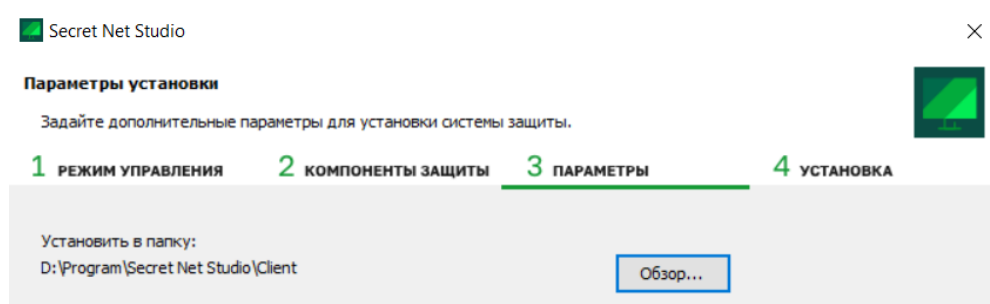


Рисунок 1.7

На рисунке 1.8 показаны этапы установки программы.

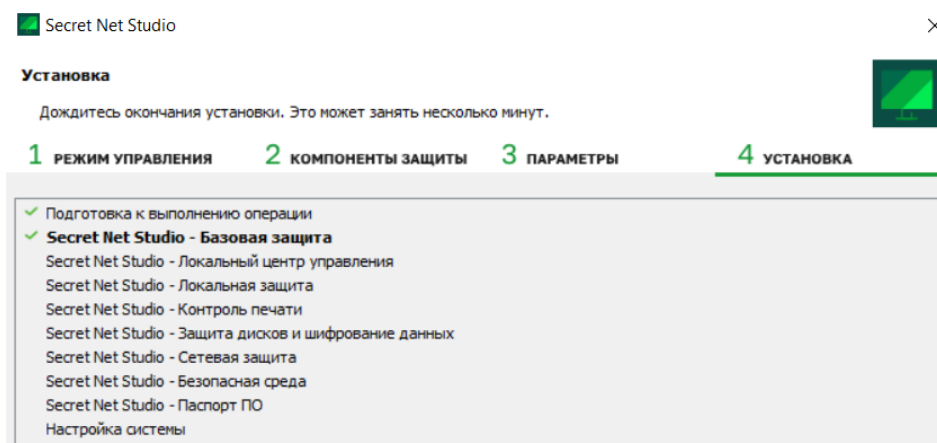


Рисунок 1.8

После установки SNS отобразилось уведомление о необходимости перезагрузки, рисунок 1.9.

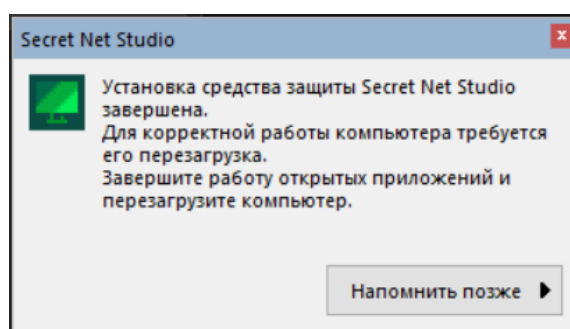


Рисунок 1.9

После перезагрузки системы, до входа в систему, выполнялась инициализация сервисов, рисунок 1.10.

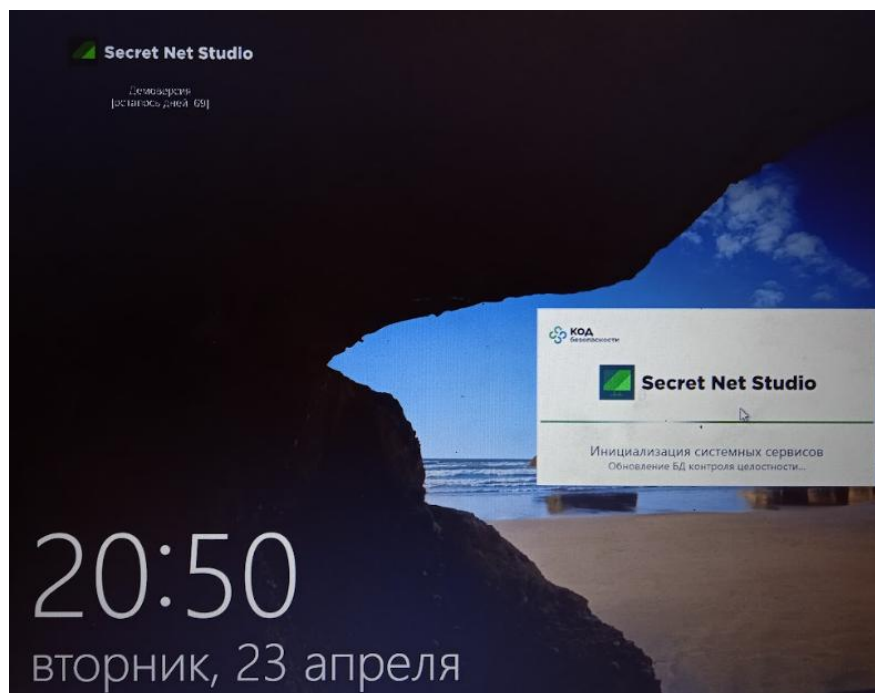


Рисунок 1.10

После входа в систему на панели задач отображалась иконка SNS, рисунок 1.11.

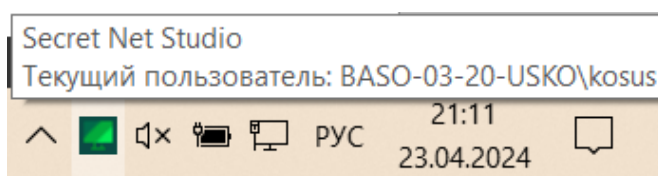


Рисунок 1.11

Программа была успешно установлена.

2 ЗАДАНИЕ №2

Настройка политик безопасности для SNS, установленного на рабочем месте пользователя автоматизированной системы в защищенном исполнении.

Ход выполнения задания

Под учётной записью администратора операционной системы было запущено приложение SNS «Центр управления», рисунок 2.1.

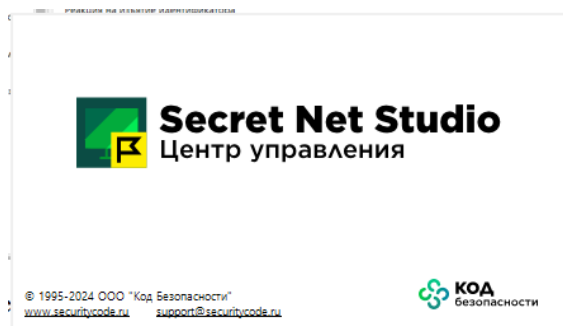


Рисунок 2.1

Согласно таблице 2.1 во вкладке «Настройки» была выполнена настройка базовой защиты, рисунки 2.2 – 2.4.

Таблица 3.1 — Критерии политики защиты информации на АРМ

Параметр настройки	Задаваемое значение
Максимальный период не активности до блокировки экрана	10 минут
Запрет вторичного входа в систему	Включено
Количество неудачных попыток аутентификации	10 попыток
Режим идентификации пользователя	По имени
Режим аутентификации пользователя	Стандартная аутентификация
Оповещение пользователя	Оповещать пользователя о последнем успешном входе в систему
Максимальный размер журнала системы защиты	4096 КБ
Политика перезаписи событий	Затирать события по мере необходимости

Параметр настройки	Задаваемое значение
Теневое копирование: Размер хранилища	15%
Перенаправление устройств в RDP-подключениях: Устройств Plug and Play	Запрещено подключать удаленные устройства к компьютеру
Перенаправление принтеров в RDP-подключениях	Запрещено использовать принтеры компьютера удаленно
Самозащита продукта	Включить

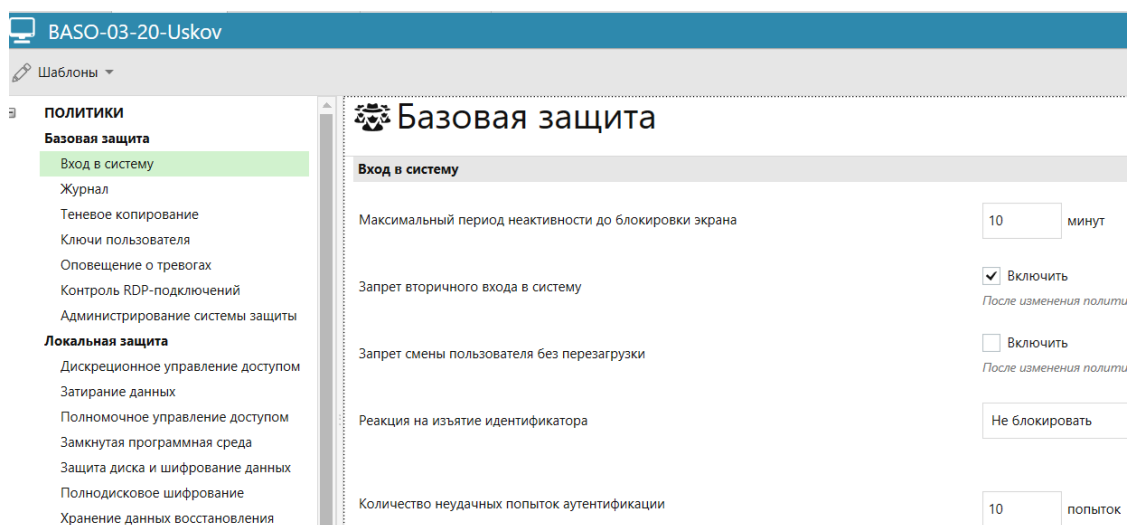


Рисунок 2.2

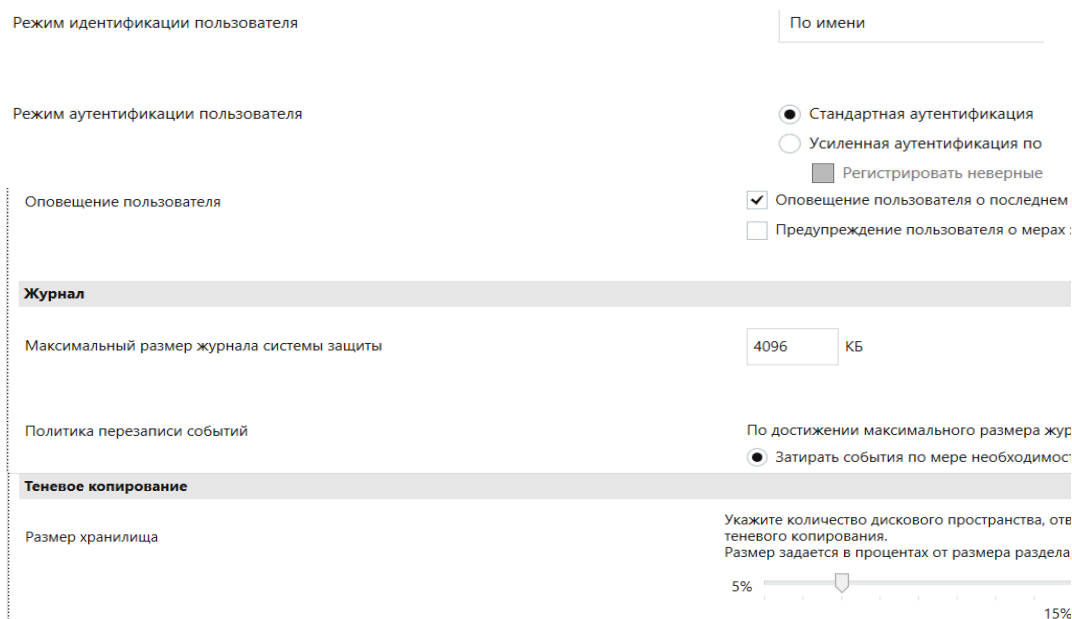


Рисунок 2.3

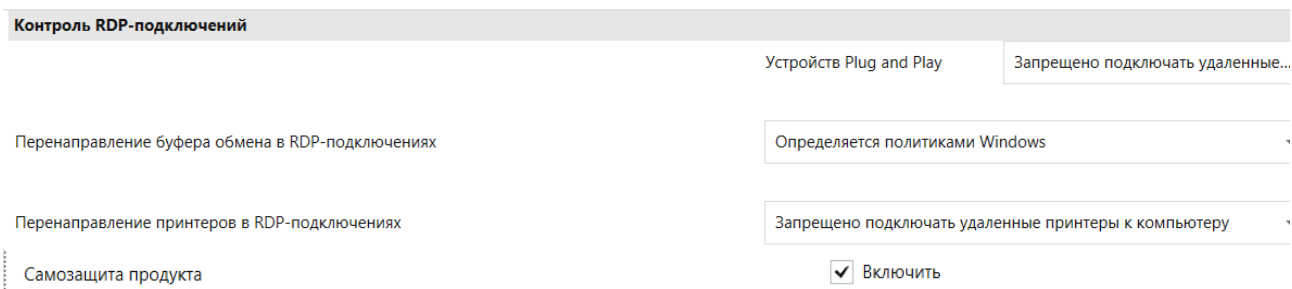


Рисунок 2.4

После внесения изменений в политику отобразилось уведомление о необходимости перезагрузки компьютера, рисунок 2.5.

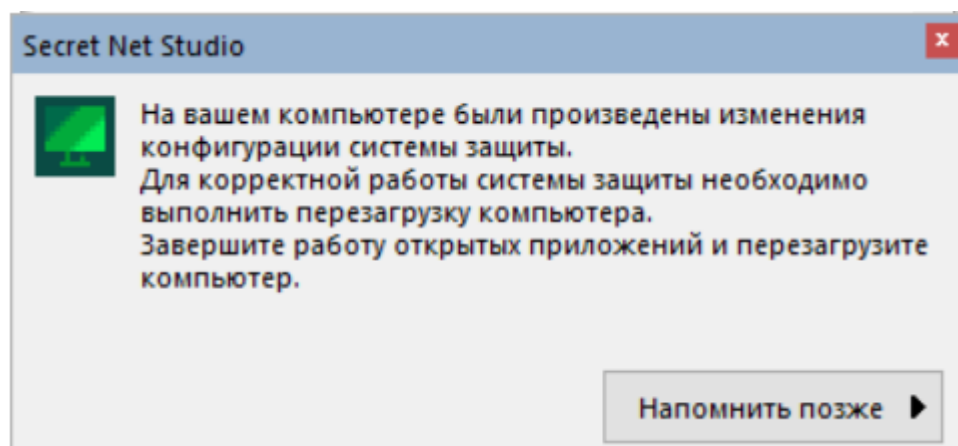


Рисунок 2.5

Была выполнена перезагрузка компьютера, настройка политики успешно применилась.

3 ЗАДАНИЕ №3

Настройка в SNS полномочного управления доступом к ресурсам рабочего места пользователя автоматизированной системы в защищенном исполнении.

Ход выполнения задания

До выполнения настройки полномочного управления доступом, контроль потоков был выключен, рисунок 3.1.

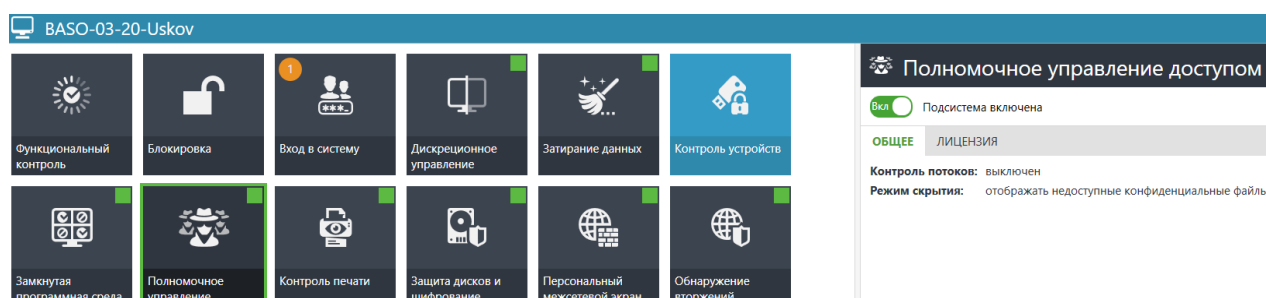


Рисунок 3.1

Пользователь korus состоит в группе администраторов системы (рисунок 3.2), поэтому настройка полномочного управления доступом для администратора была выполнена для этого пользователя.

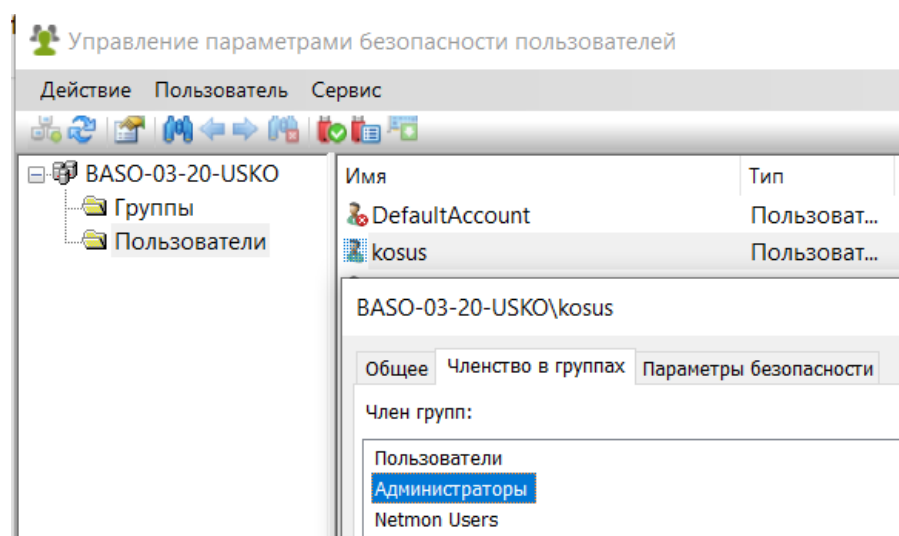


Рисунок 3.2

Для администратора был установлен самый высокий уровень доступа – «Строго конфиденциально», рисунок 3.3. По мимо этого ему было позволено управлять категориями конфиденциальности.

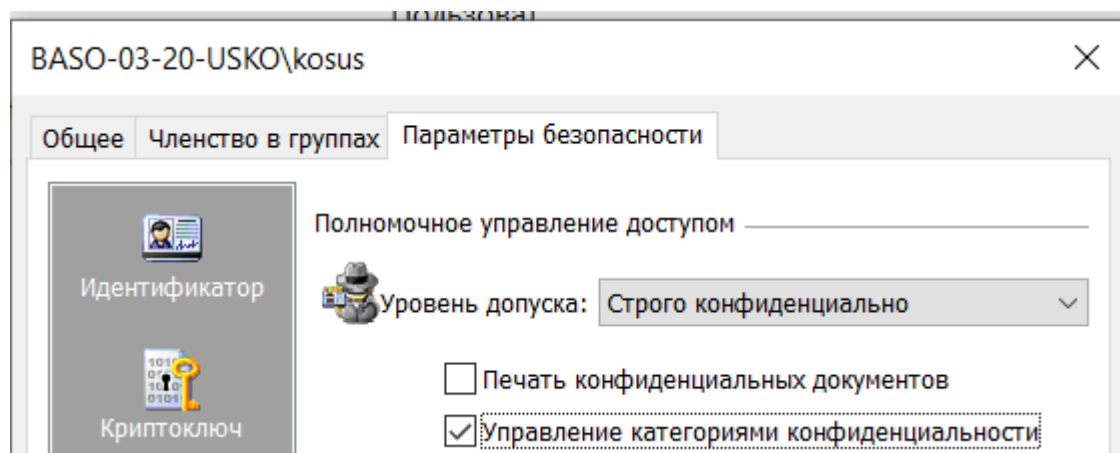


Рисунок 3.3

На локальном диске С был создан каталог «Усков», а нём – «Конфиденциально», «Не конфиденциально» и «Строго конфиденциально». Для каждого каталога из «Усков» была установлена категория конфиденциальности соответствующая названию, рисунок 3.4.

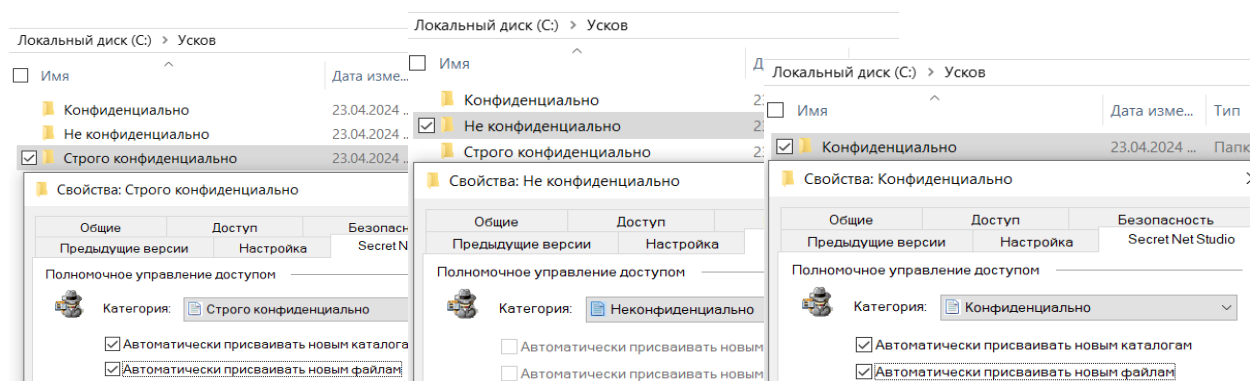


Рисунок 3.4

С помощью приложения SNS «Управление пользователями», вкладка «Пользователь» (рисунок 3.5), были созданы 3 пользователя с паролями «123» и необходимыми уровням допуска, рисунки 3.6 – 3.8.

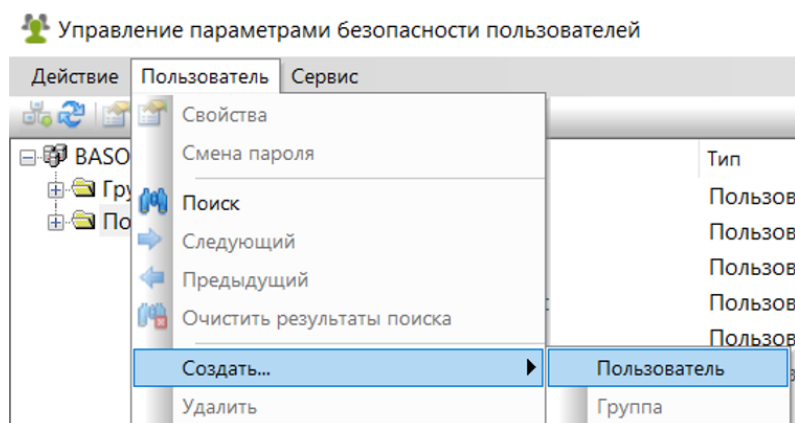


Рисунок 3.5

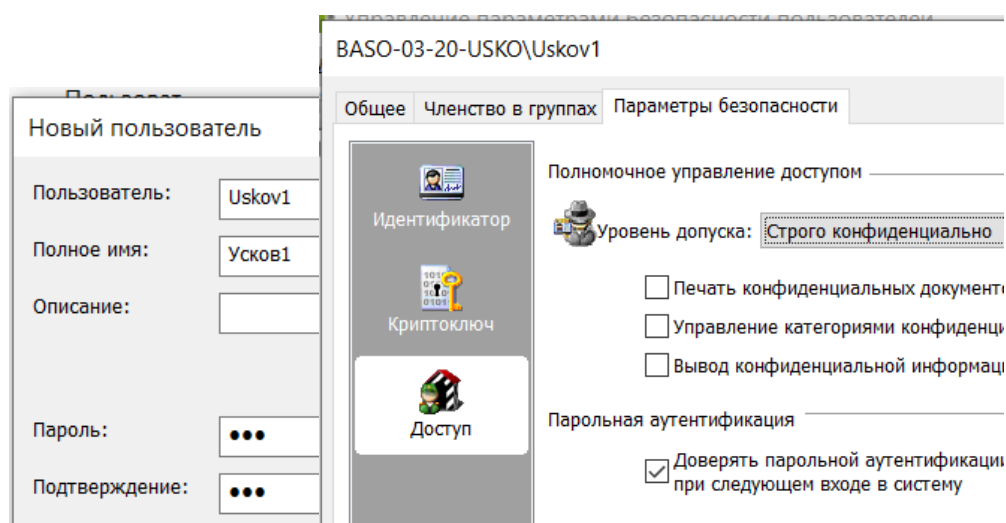


Рисунок 3.6

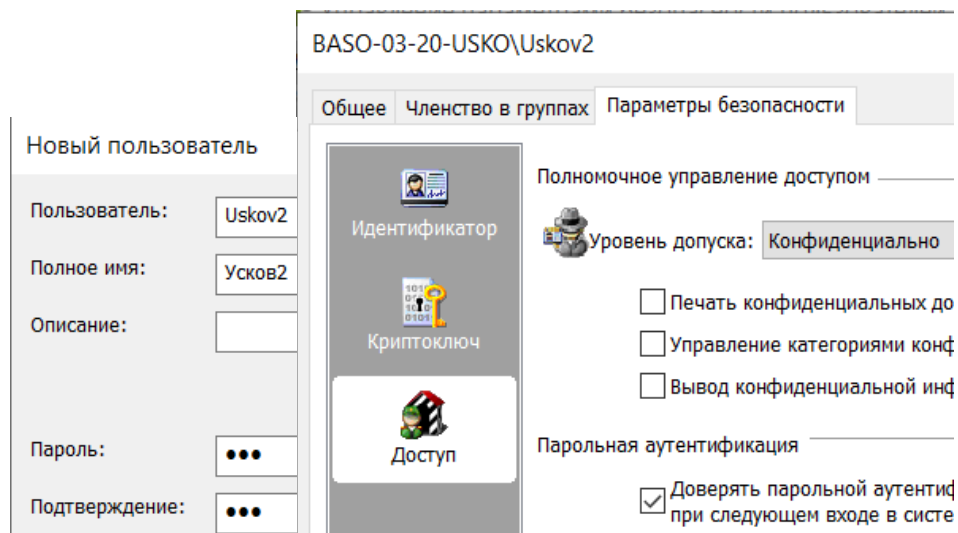


Рисунок 3.7

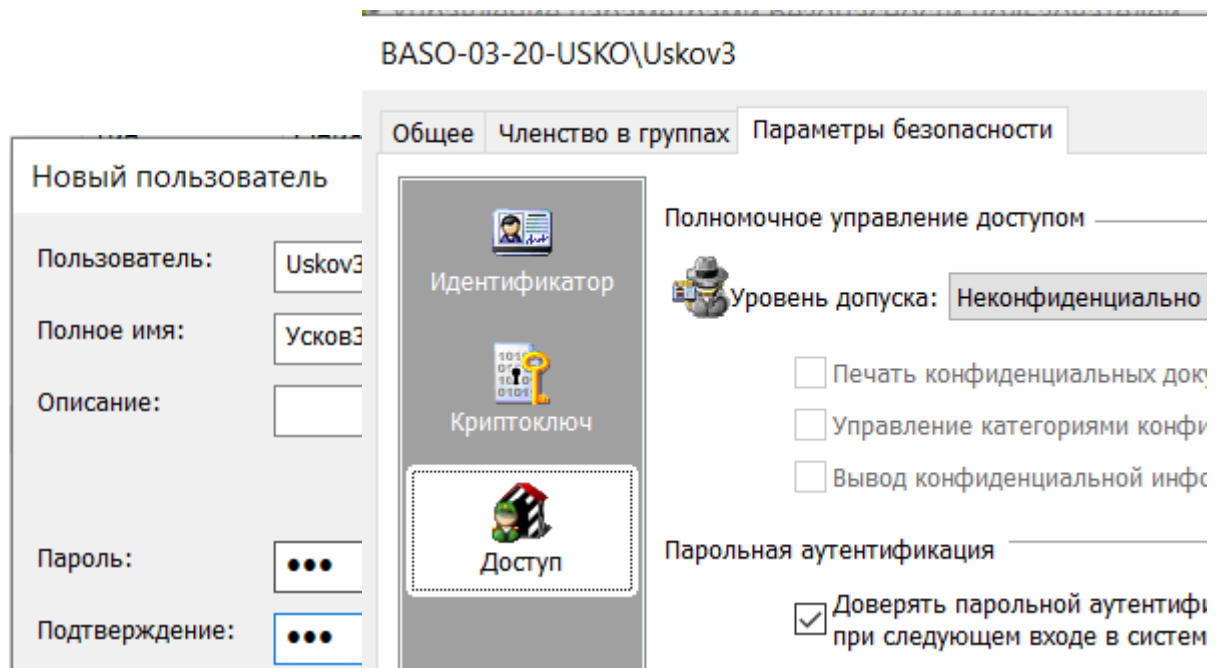


Рисунок 3.8

С помощью мастера установки была выполнена установка LibreOffice версии 7.4.5.1, рисунок 3.9.

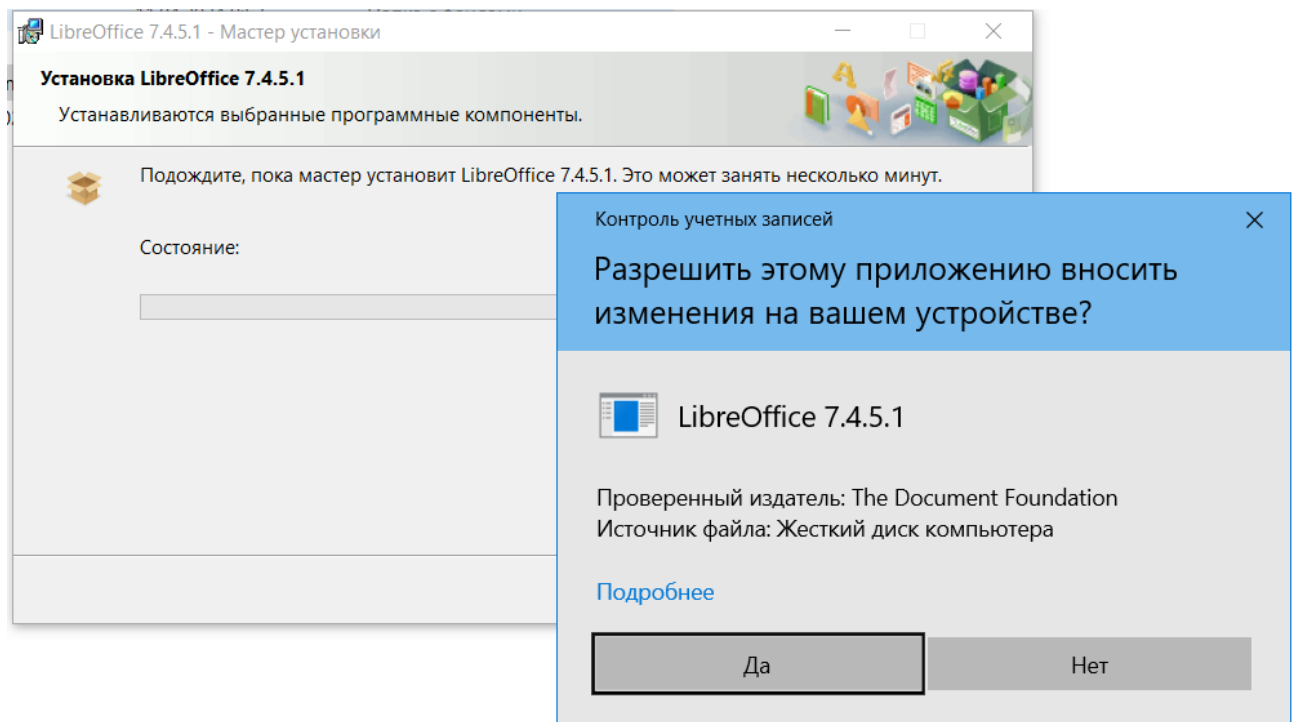


Рисунок 3.9

В созданном ранее каталоге «Усков» с помощью LibreOffice были созданы необходимые текстовые файлы и электронные таблицы, рисунок 3.10.

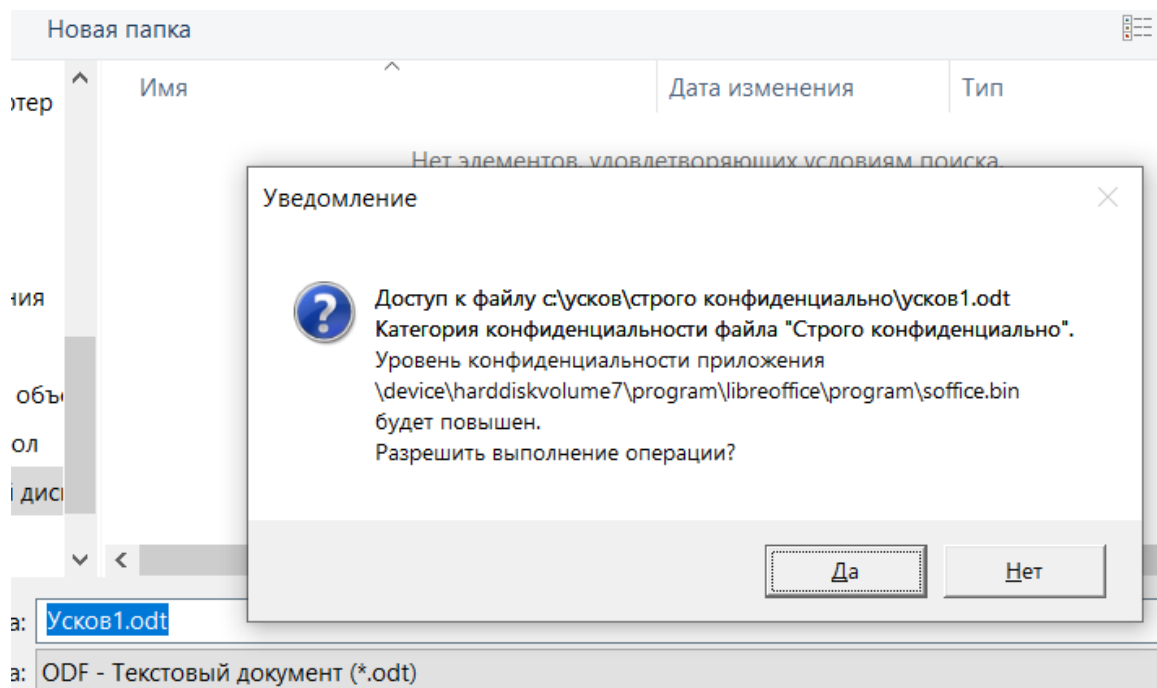


Рисунок 3.10

С помощью программы по управлению полномочным доступом, было настроено правило приложения LibreOffice для перенаправления, рисунок 3.11.

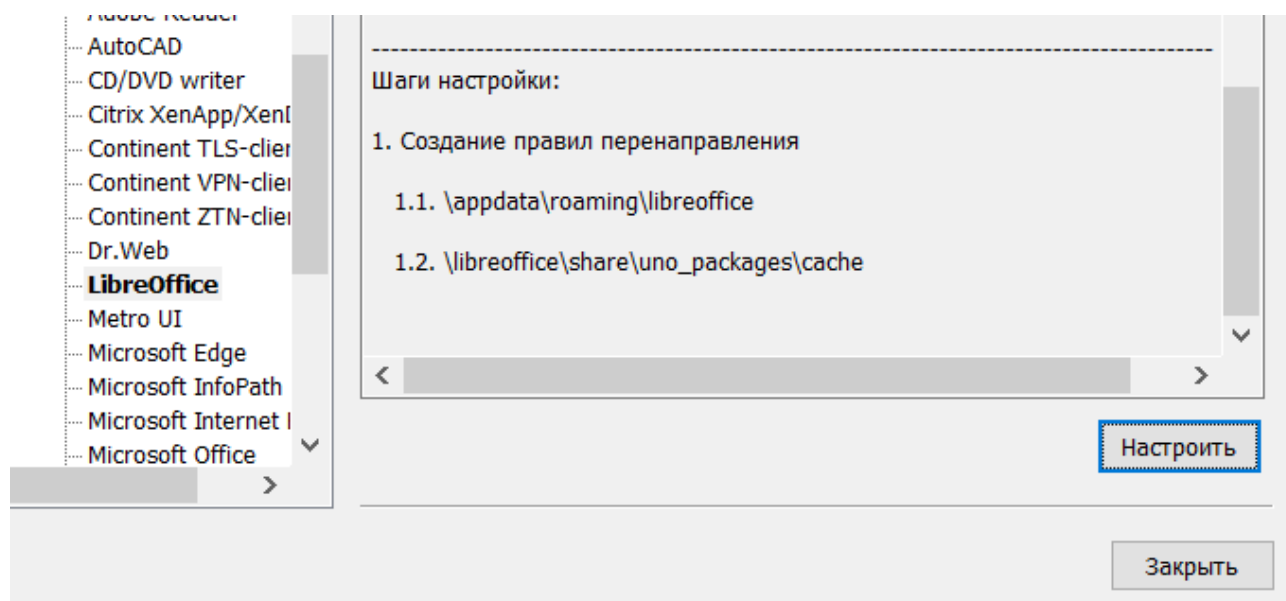


Рисунок 3.11

Затем в локальном центре управление SNS был включен контроль потоков для полномочного управления доступом (рисунок 3.12), а компьютер был перезапущен.

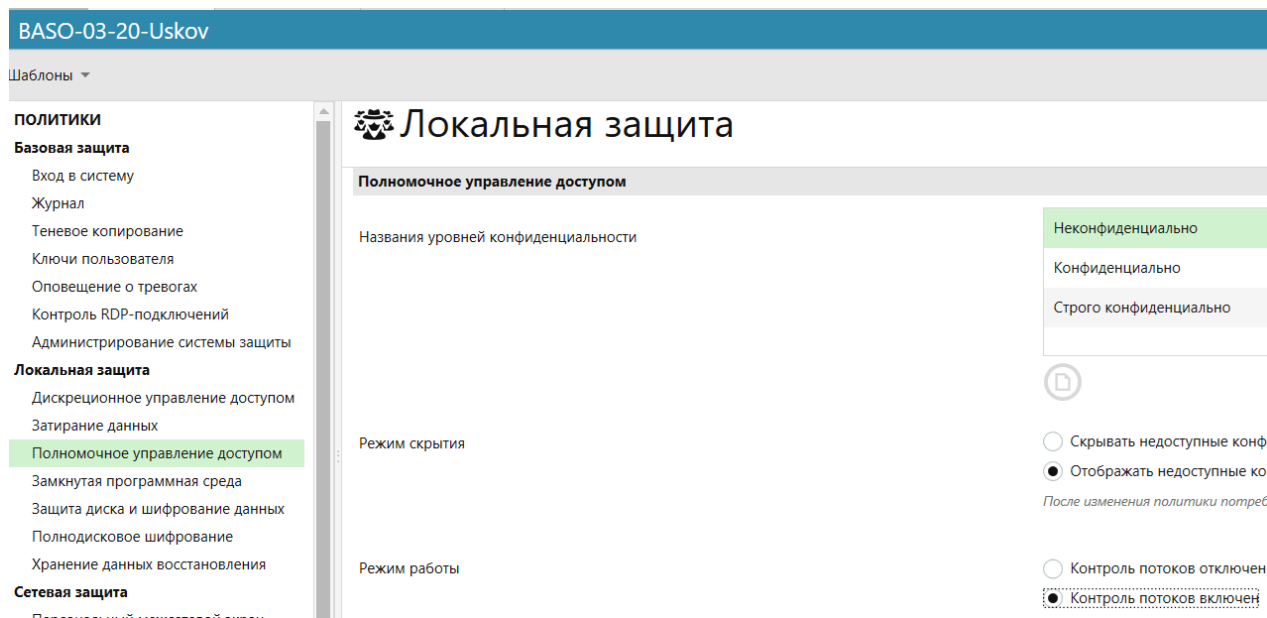


Рисунок 3.12

После перезагрузки системы был выполнен вход под учётной записью «Усков3». При попытке открыть текстовые файлы или электронные таблицы от приложения LibreOffice с уровнем допуска выше «Не конфиденциально», отображались ошибки, рисунок 3.13.

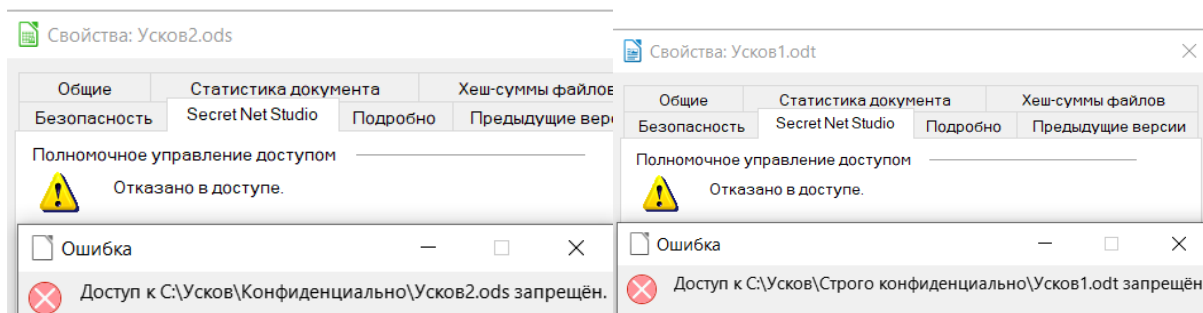


Рисунок 3.13

Затем был выполнен вход под учётной записью «Усков2», а уровень конфиденциальности для сеанса установлен на «Конфиденциально», рисунок 3.14.

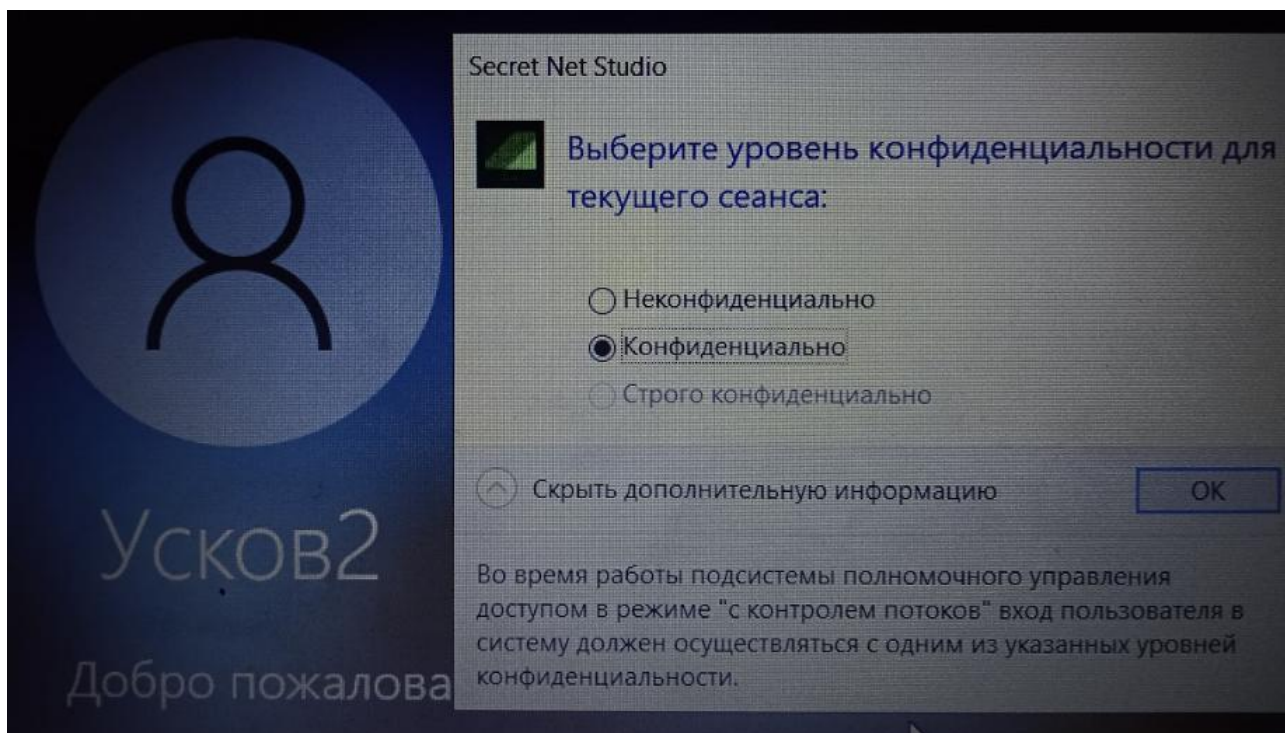


Рисунок 3.14

При попытке открыть текстовый файл или электронную таблицу с уровнем допуска ниже «Конфиденциально», отображалась ошибка о невозможности их редактирования. А открытие файлов от LibreOffice с уровнем допуска выше «Конфиденциально» было невозможным. Соответствующие ошибки представлены на рисунке 3.15.

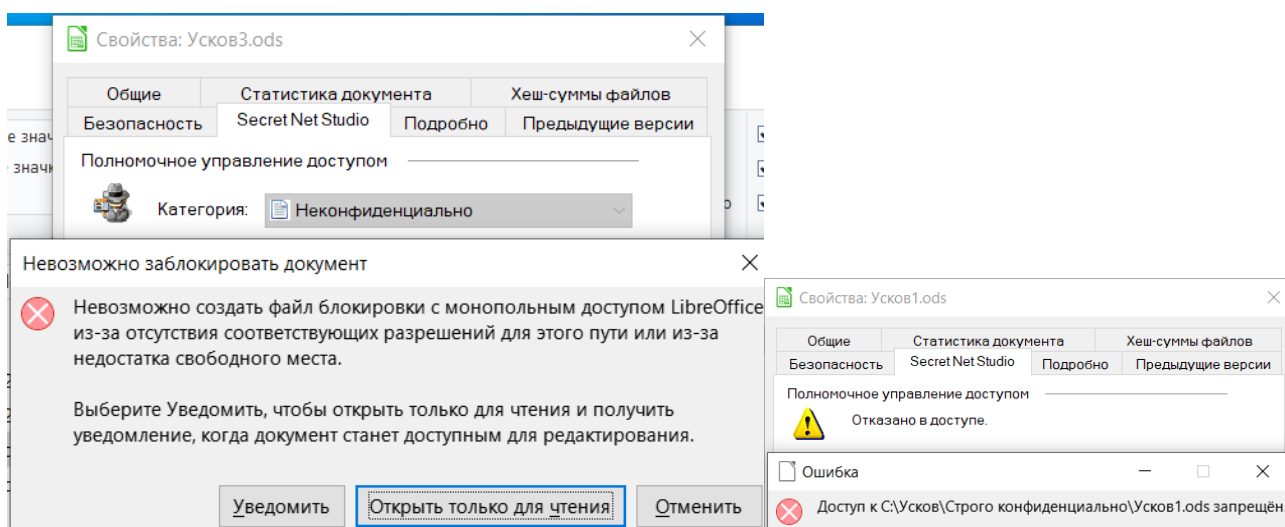


Рисунок 3.15

После был выполнен вход под учётной записью «Усков1» с уровнем «Строго конфиденциально» для сеанса, рисунок 3.16.

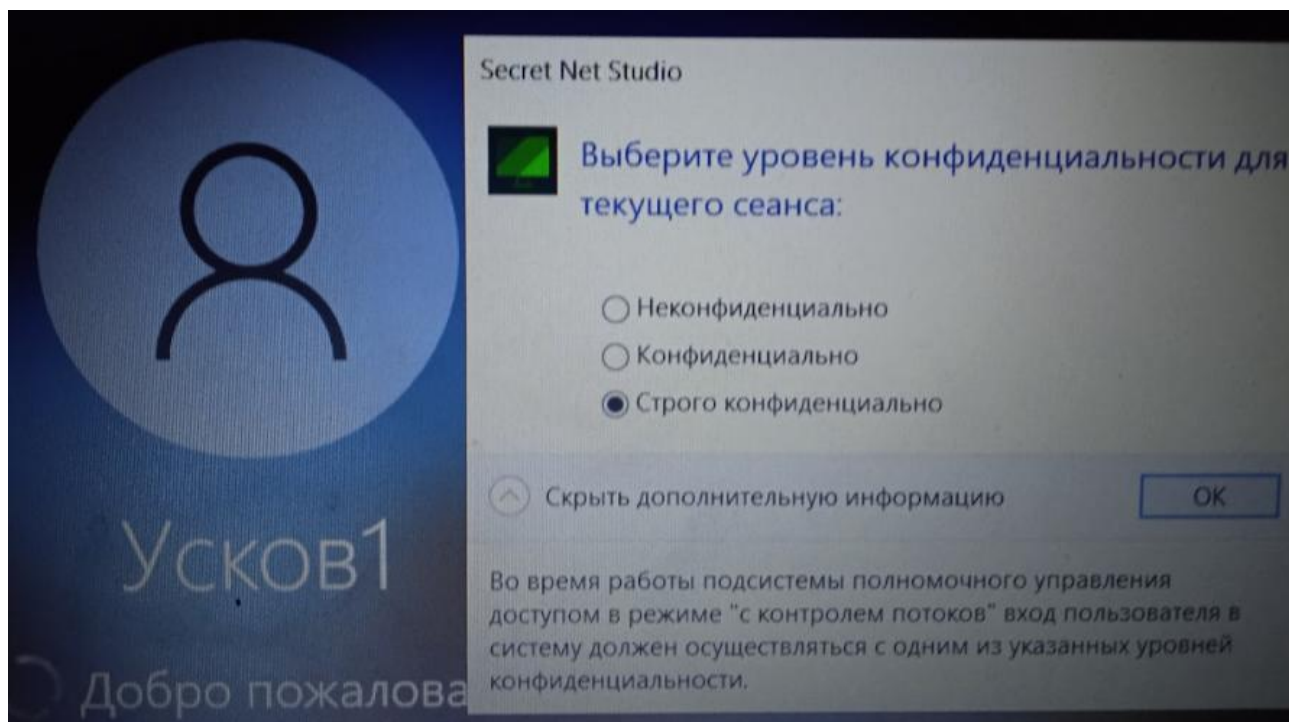


Рисунок 3.16

При попытке открыть текстовые файлы или электронные таблицы с уровнем допуска ниже «Строго конфиденциально» отображалась ошибка о невозможности редактирования файла, что отображено на рисунке 3.17.

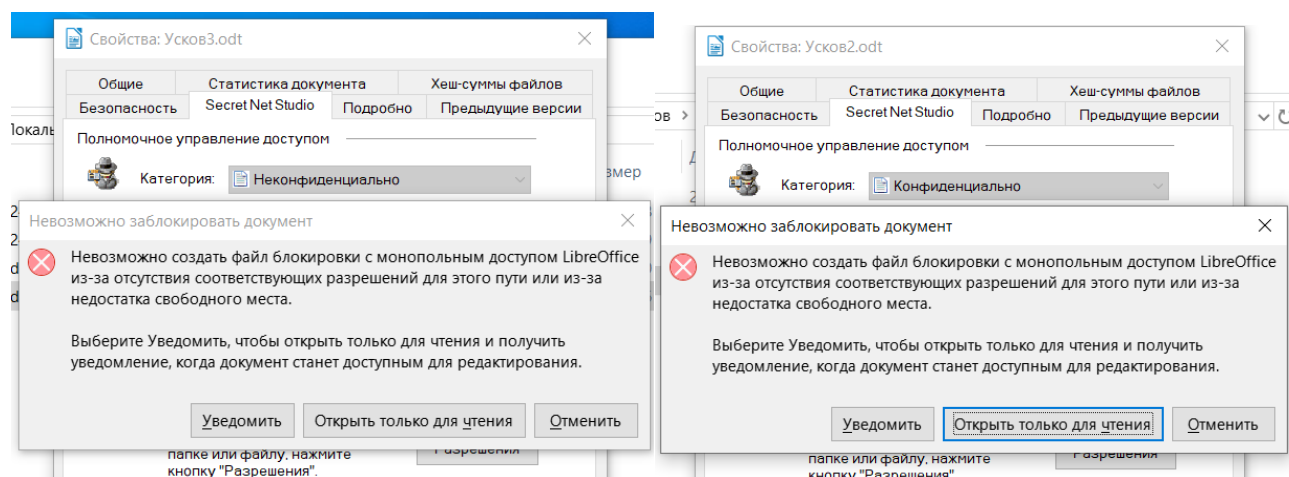


Рисунок 3.17

В результате авторизации под учётным записями с различным уровнем допуска, была установлена корректная работа полномочного управление допуском, а именно пользователь с уровнем допуска выше, чем у файла не мог вносить в него изменения, а если его уровень допуска был ниже, то вовсе не мог открыть файл.

4 ЗАДАНИЕ №4

Настройка аудита операционной системы рабочего места автоматизированной системы и событий SNS.

Ход выполнения задания

С помощью приложения SNS «Локальный центр управления» размер журнала был увеличен до 20480 КБ, рисунок 4.1.

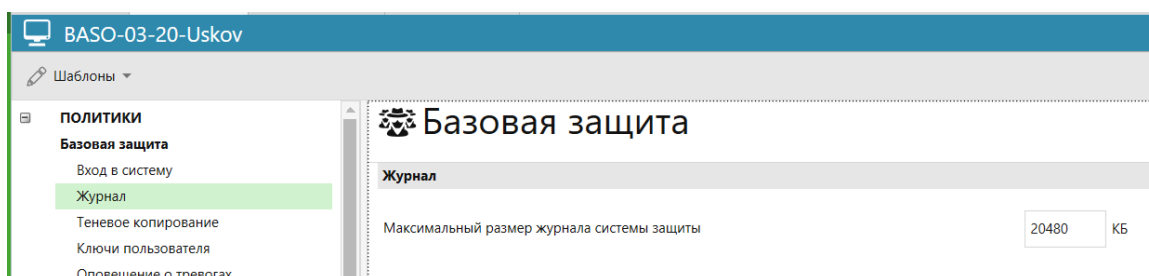


Рисунок 4.1

В разделе «РЕГИСТРАЦИЯ СОБЫТИЙ» для групп «Администрирование», «Администрирование системы защиты», «Вход в систему» был установлен аудит успеха и отказа. Для остальных групп установлен аудит отказа и отменён аудит успеха. Остальные параметры, не относящиеся к аудиту успеха или отказа, были установлены или отменены в соответствии с требованиями к аудиту событий на АРМ. Часть установленных параметров отображена на рисунках 4.2 – 4.7.

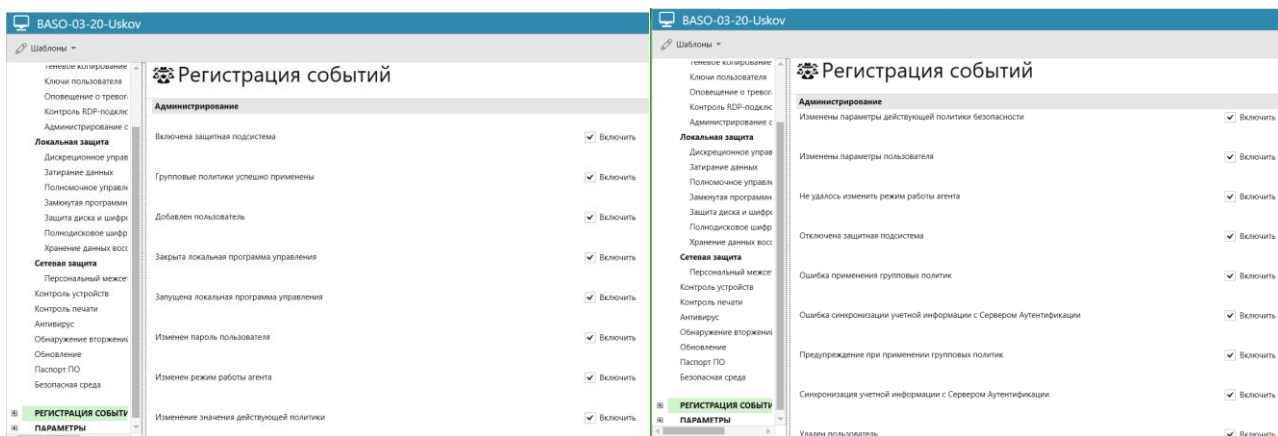


Рисунок 4.2

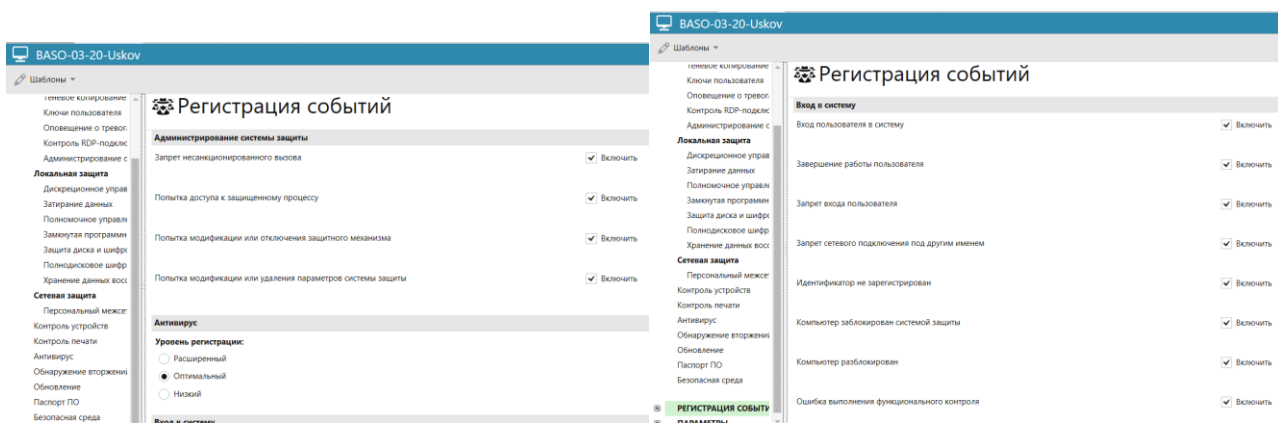


Рисунок 4.3

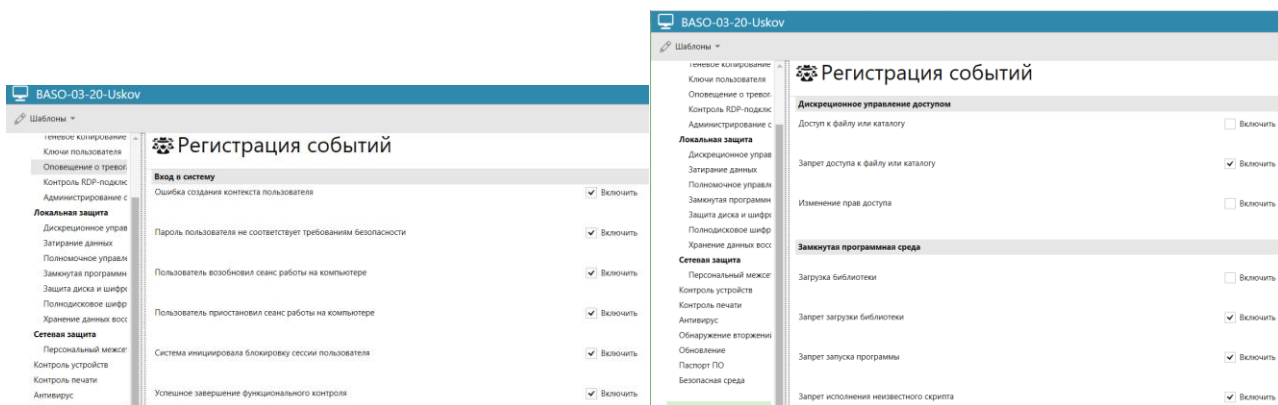


Рисунок 4.4

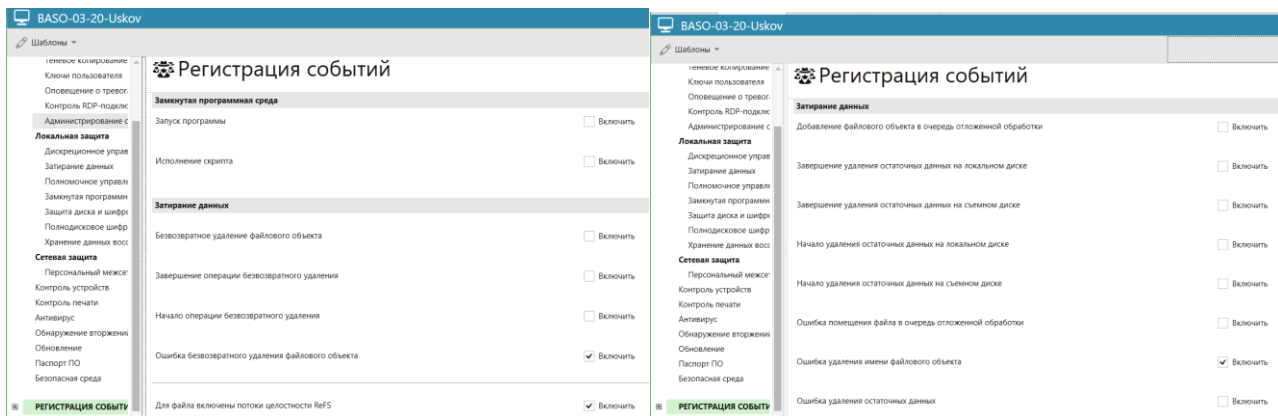


Рисунок 4.5

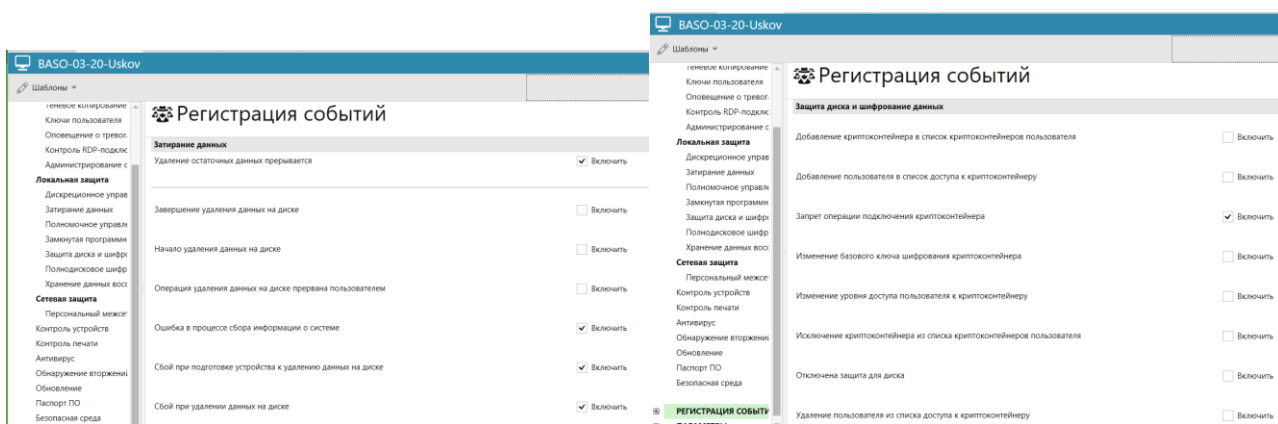


Рисунок 4.6

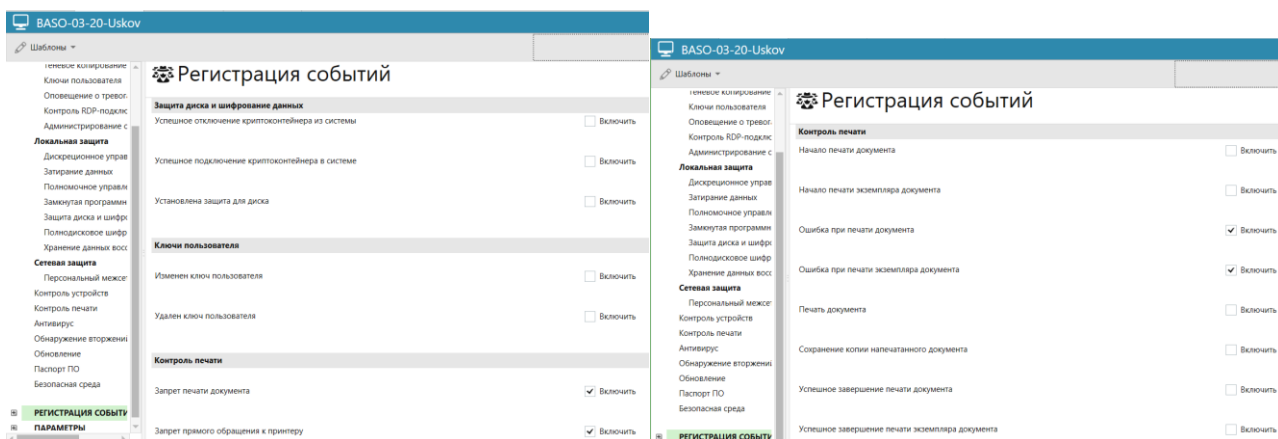


Рисунок 4.7

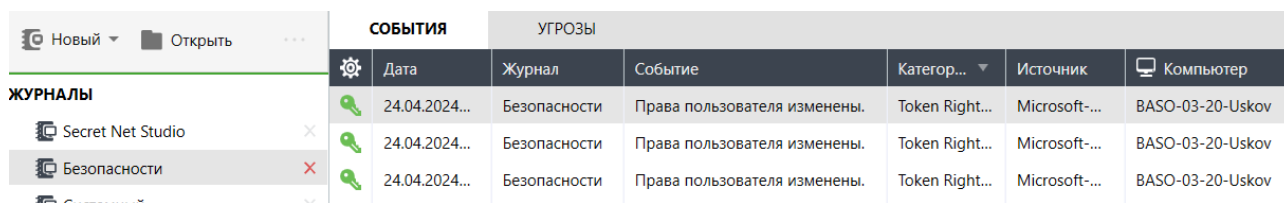
После выполнения настроек, для их применения, компьютер был переза-
пущен.

5 ЗАДАНИЕ №5

Работа с журналом событий SNS, установленного на рабочем месте пользователя автоматизированной системы.

Ход выполнения задания

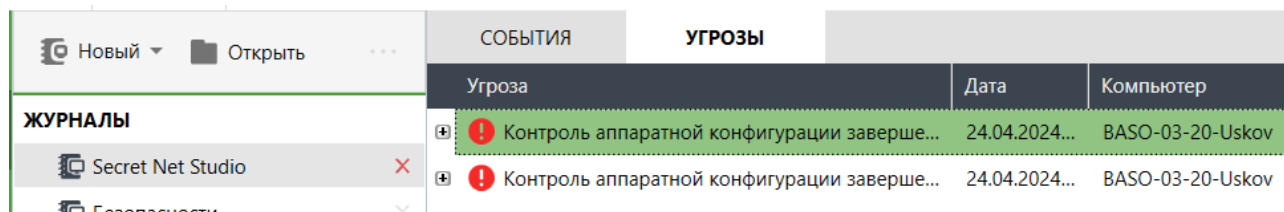
С помощью приложения SNS «Локальный центр управления» поочередно были загружены журналы «Secret Net Studio», «Безопасности», «Системный» и «Приложений». Журнал безопасности показан на рисунке 5.1.



ЖУРНАЛЫ	СОБЫТИЯ		УГРОЗЫ				
	Диагностика	Дата	Журнал	Событие	Категор...	Источник	Компьютер
Secret Net Studio	✕	24.04.2024...	Безопасности	Права пользователя изменены.	Token Right...	Microsoft...	BASO-03-20-Uskov
Безопасности	✕	24.04.2024...	Безопасности	Права пользователя изменены.	Token Right...	Microsoft...	BASO-03-20-Uskov
Системный	✓	24.04.2024...	Безопасности	Права пользователя изменены.	Token Right...	Microsoft...	BASO-03-20-Uskov

Рисунок 5.1

Затем были просмотрены угрозы для журнала «Secret Net Studio», рисунок 5.2.



ЖУРНАЛЫ	СОБЫТИЯ		УГРОЗЫ		
	Диагностика	Дата	Угроза	Дата	Компьютер
Secret Net Studio	✕	24.04.2024...	Контроль аппаратной конфигурации заверше...	24.04.2024...	BASO-03-20-Uskov
Безопасности	✓	24.04.2024...	Контроль аппаратной конфигурации заверше...	24.04.2024...	BASO-03-20-Uskov

Рисунок 5.2

Аналогично имеющимся журналам, был рассмотрен запрос из журналов по существующему фильтру «Все тревоги», рисунок 5.3.

Аналогично был создан фильтр для просмотра записей пользователя «Uskov1» и отображены сами записи, рисунок 5.6.

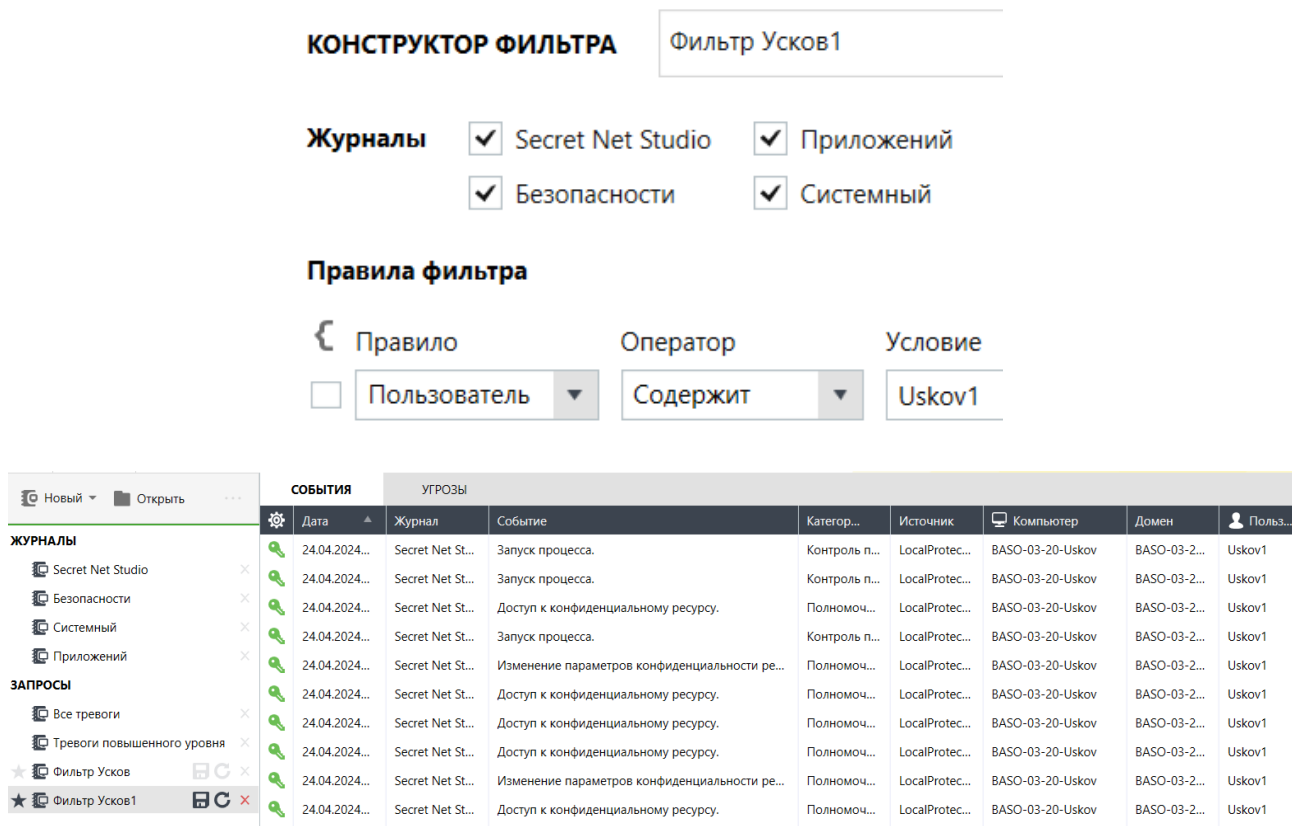


Рисунок 5.6

В результате были рассмотрены имеющиеся журналы и подготовлены за-
просы к ним по необходимым требованиям. Программа была закрыта.

6 ЗАДАНИЕ №6

Настройка механизма дискреционного управления доступом к файлам рабочего места пользователя автоматизированной системы в защищенном исполнении.

Ход выполнения задания

На локальном диске С были созданы необходимые каталоги, рисунок 6.1. В каталогах были созданы текстовые документы.

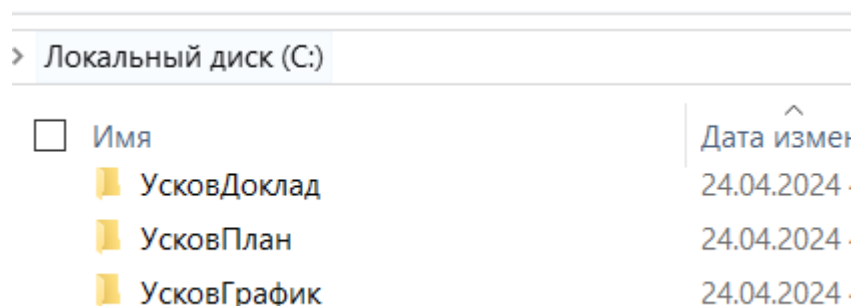


Рисунок 6.1

Используя приложение SNS «Локальный центр управления», для управления дискреционным доступом был добавлен пользователь korus, несмотря на то, что он входит в группу администраторов, рисунок 6.2.

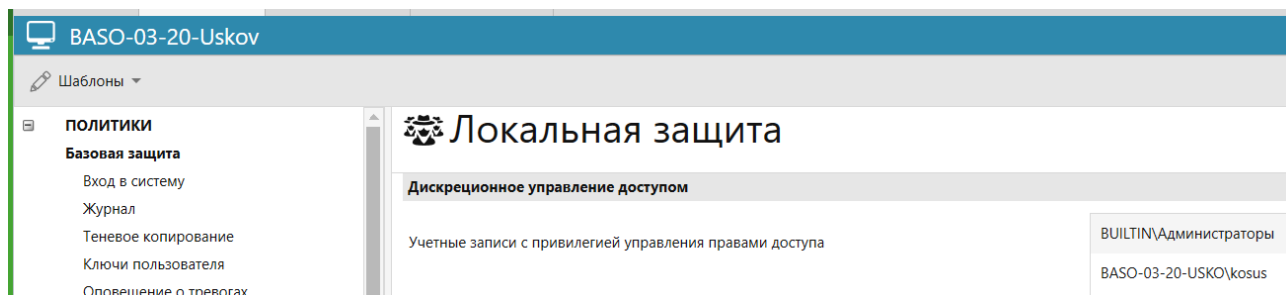


Рисунок 6.2

Были изменены настройки для ведения журнала по дискреционному управлению доступа, рисунок 6.3.

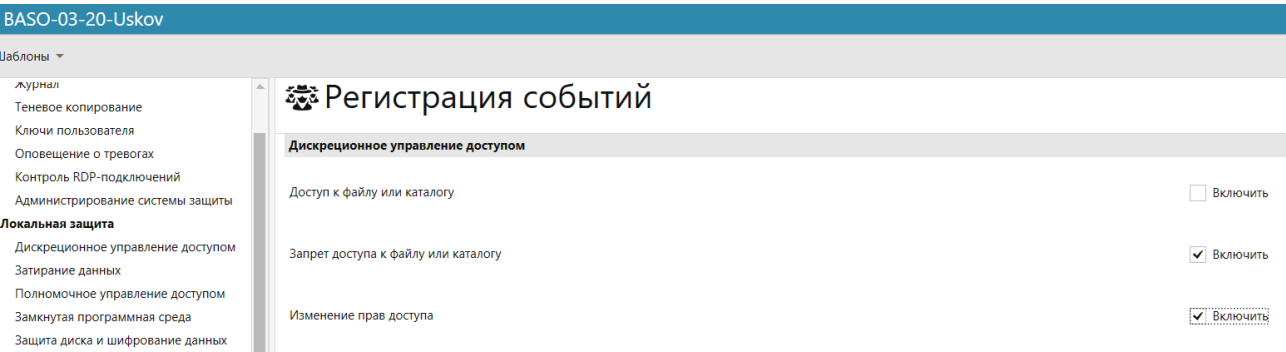


Рисунок 6.3

Затем были выполнены необходимые настройки по дискреционному доступу для созданных каталогов, рисунки 6.4 – 6.5 для «УсковДоклад», рисунки 6.6 – 6.7 для «УсковПлан» и рисунки 6.8 – 6.9 для «УсковГрафик».

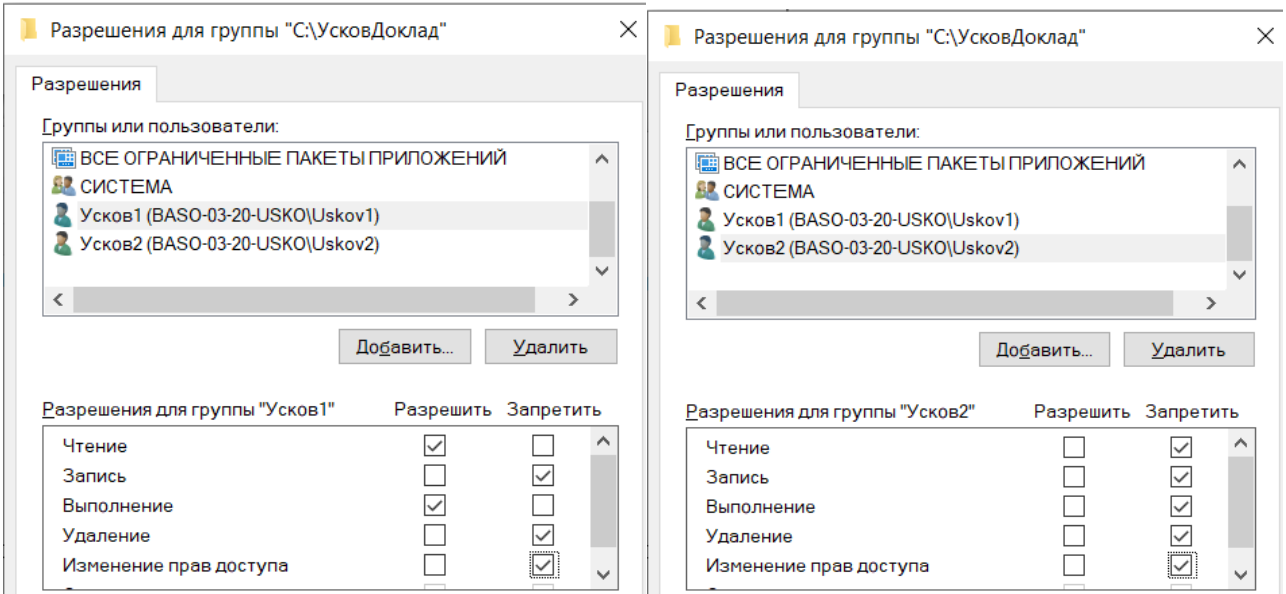


Рисунок 6.4

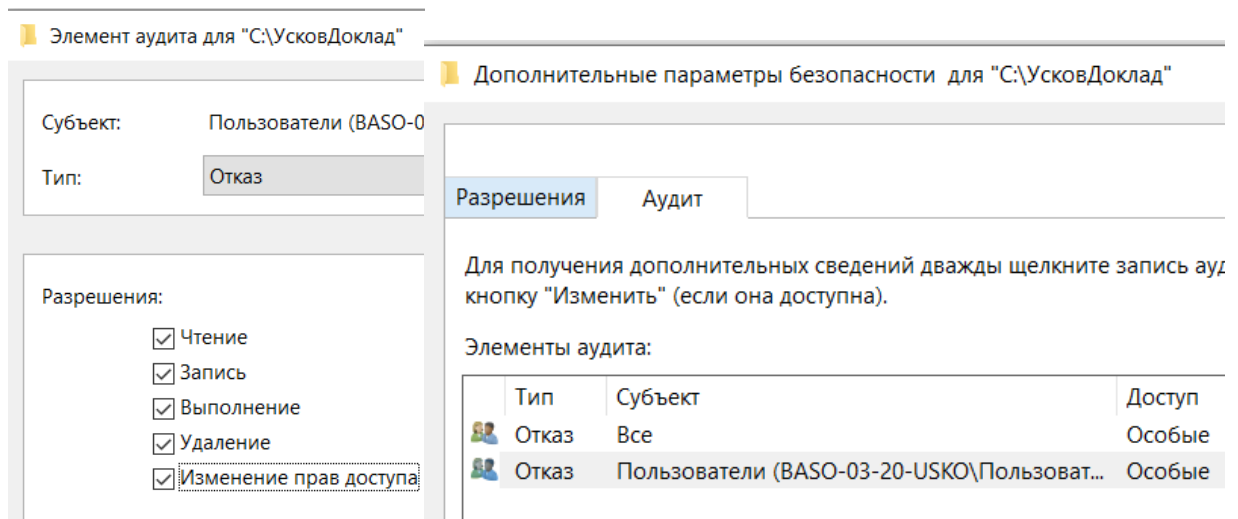


Рисунок 6.5

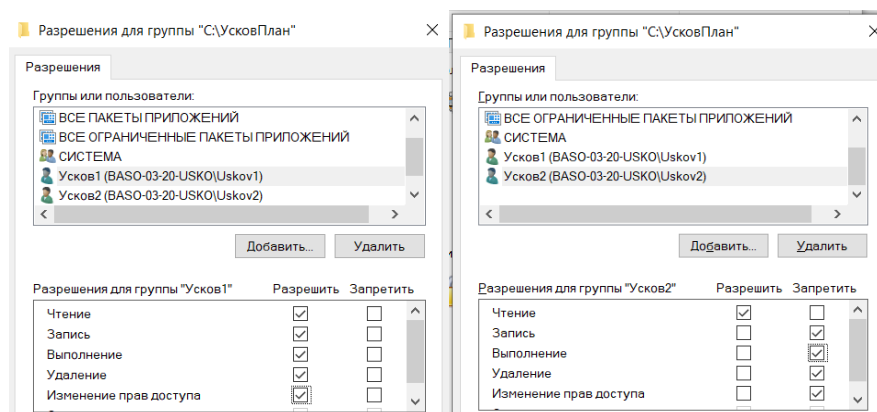


Рисунок 6.6

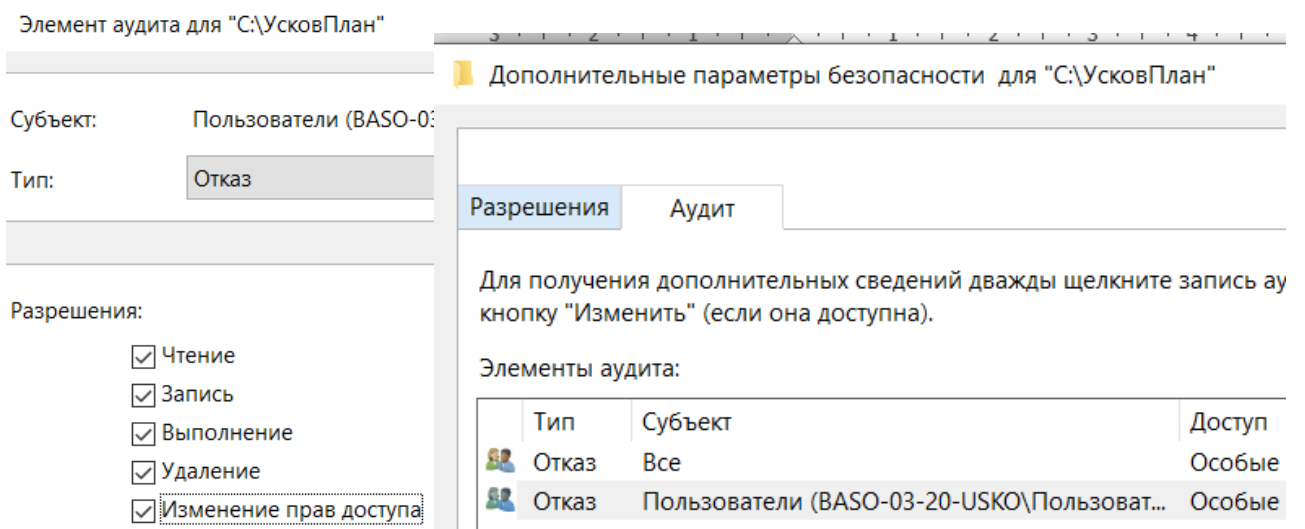


Рисунок 6.7

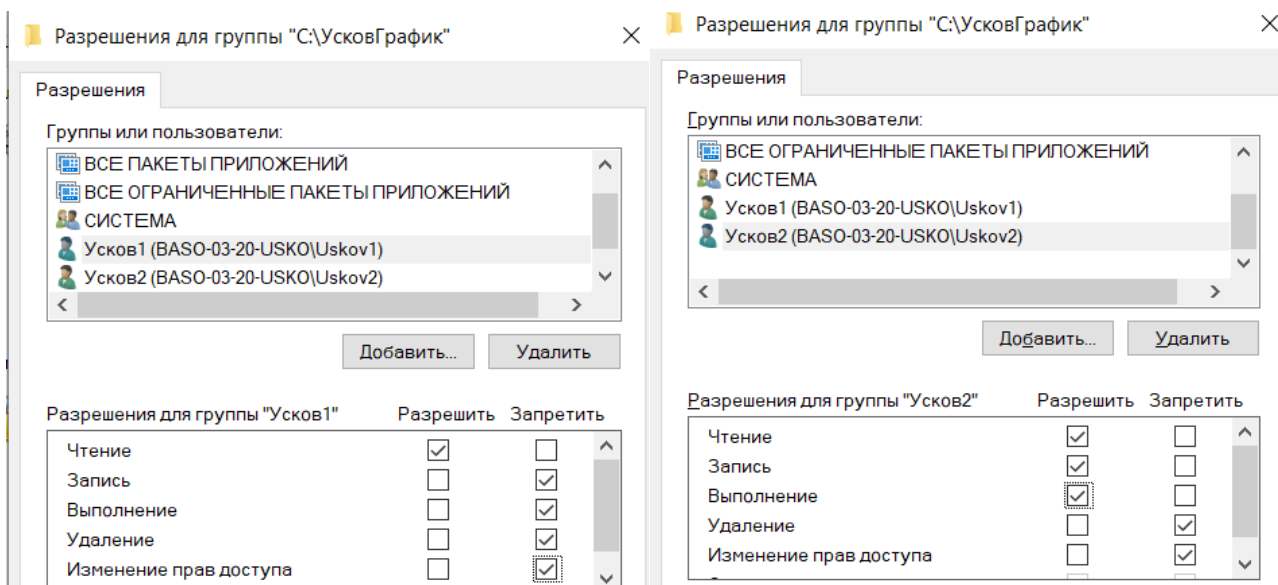


Рисунок 6.8

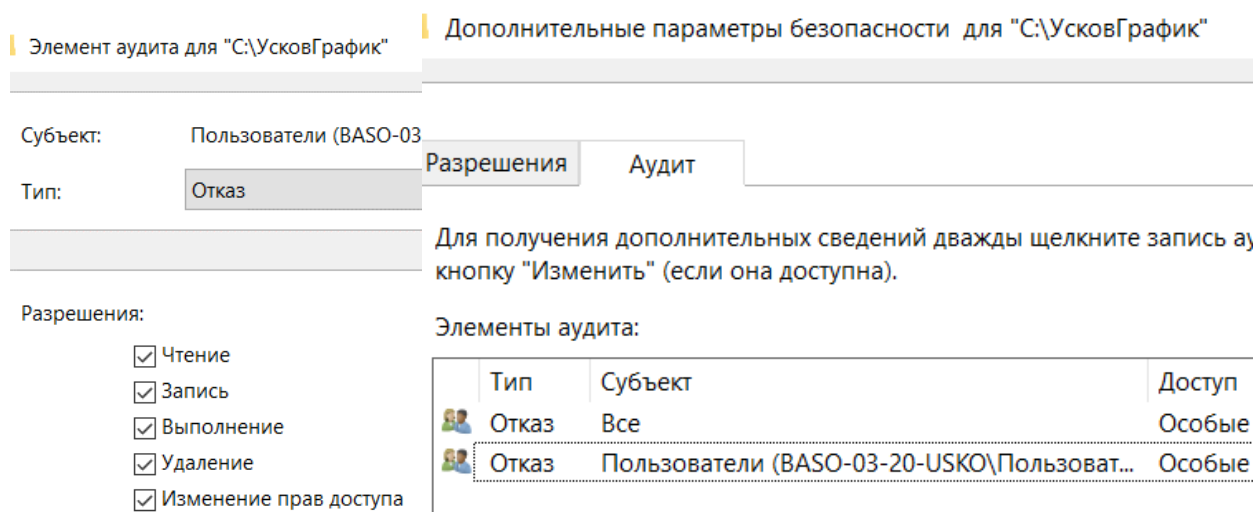


Рисунок 6.9

Для каждого текстового файла, в свойствах Secret Net Studio было проверено, что дискреционное управление доступом наследуется от родительского объекта. Т.е. настройки каталогов выполненные ранее справедливы для текстовых документов. Затем в журнале был подготовлен запрос на просмотр событий связанных с дискреционным доступом и аудитов отказа, рисунок 6.10.

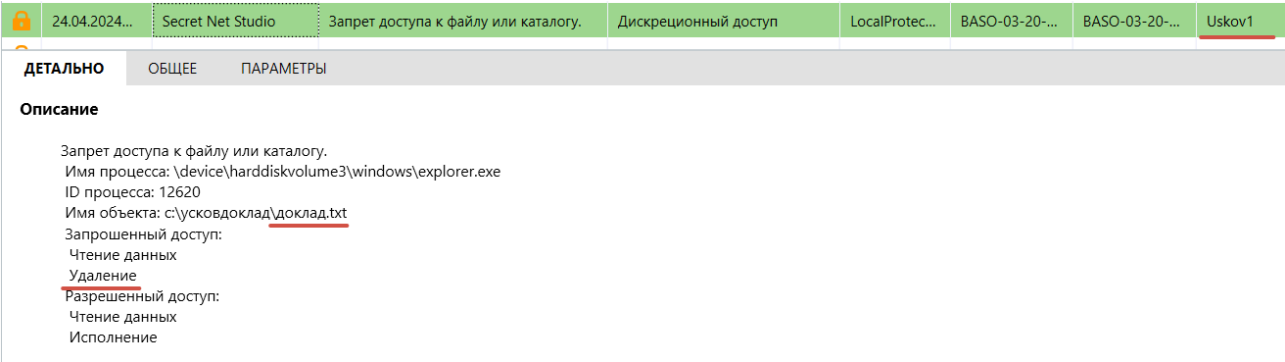


Рисунок 6.12

Пользователю Uskov1 запрещено исполнение, изменение и чтение для файлов из каталога УсковГрафик, поскольку разрешённый допуск – чтение данных, рисунок 6.13.

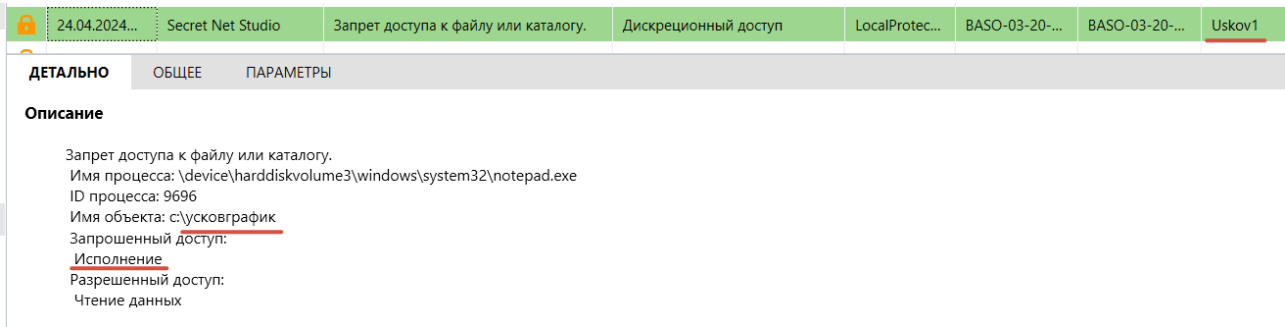


Рисунок 6.13

По рисунку 6.14 можно заметить, что пользователю Uskov2 не разрешен какой-либо допуск к файлам каталога УсковДоклад – N/A.

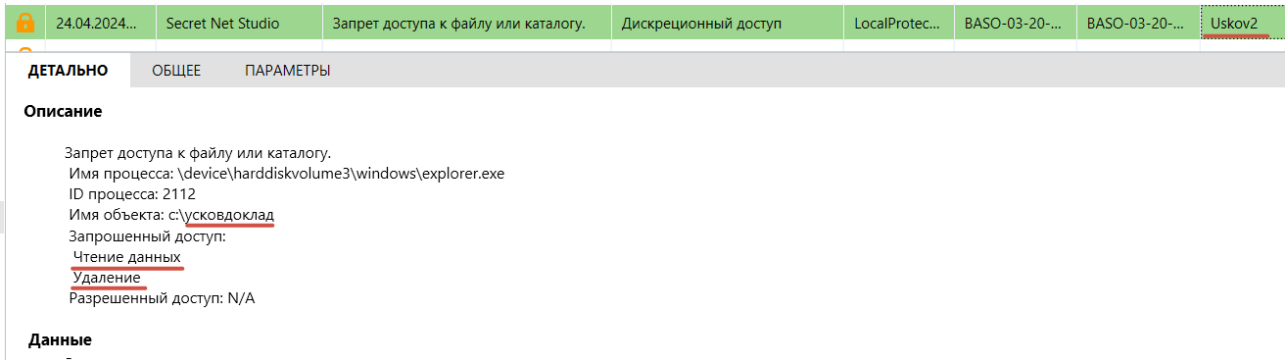


Рисунок 6.14

Пользователю Uskov2 запрещено удалять файл график.txt – рисунок 6.15.

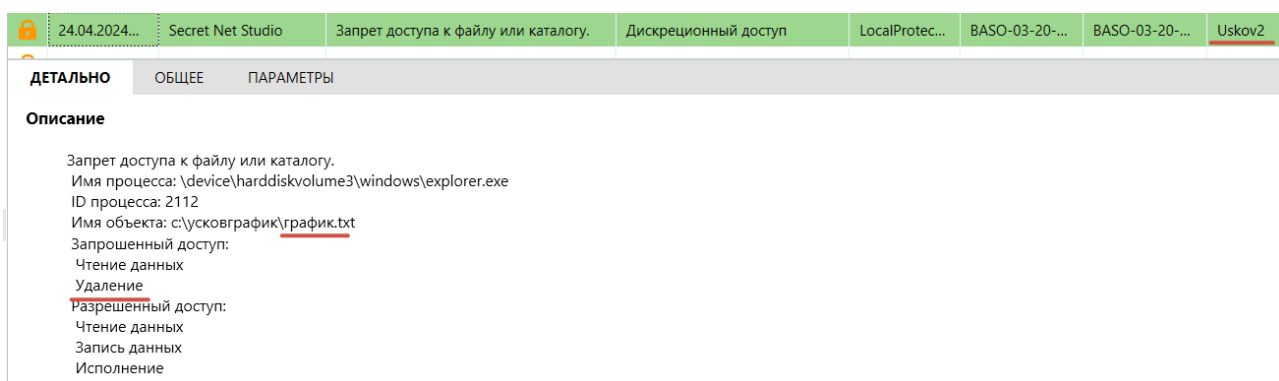


Рисунок 6.15

Пользователю Uskov2 запрещено исполнение, изменение и чтение для файлов из каталога УсковПлан, поскольку разрешённый допуск – чтение данных, рисунок 6.16.

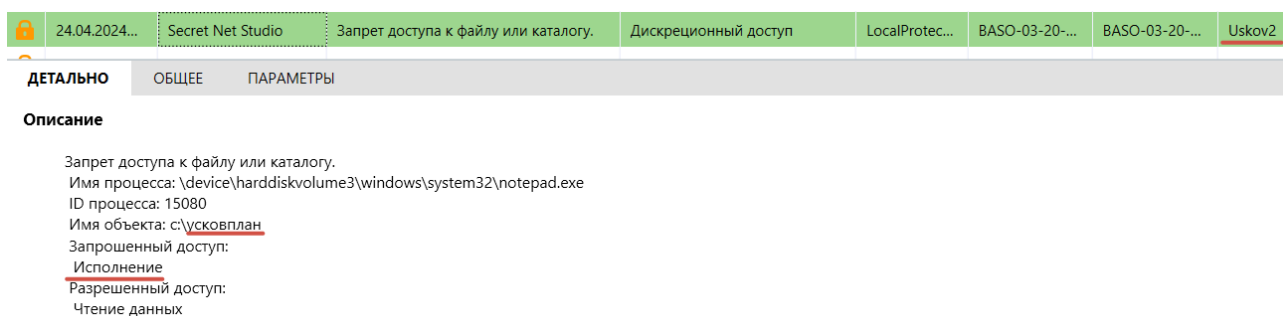


Рисунок 6.16

Проверенный записи журнала подтверждают корректную настройку дискреционного допуска.

7 ЗАДАНИЕ №7

Управление доступом к подключаемым USB-флеш-накопителям на рабочем месте пользователя автоматизированной системы в защищенном исполнении.

Ход выполнения задания

Для выбранного USB устройства, в разделе «Контроль устройств» приложения SNS «Локальный центр управления», была выполнена базовая настройка по допуску – рисунок 7.1.

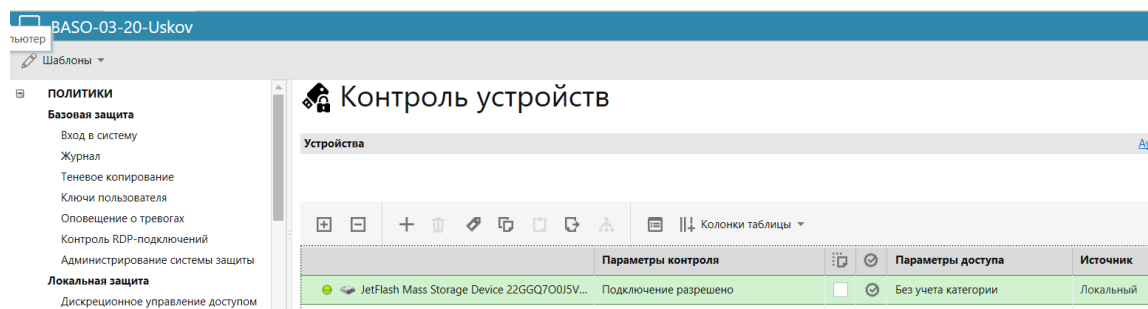


Рисунок 7.1

Затем для выбранного USB устройства по хранению данных был установлен полный запрет для пользователя Uskov2 – рисунок 7.2.

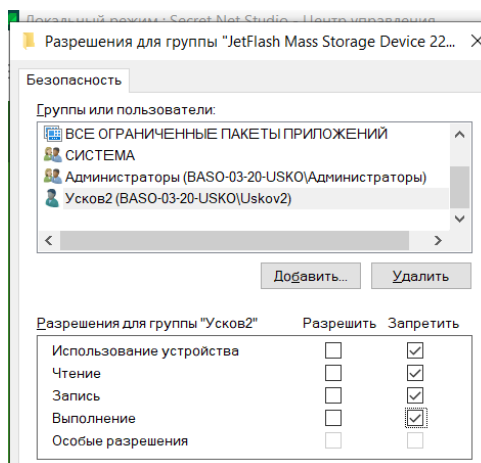


Рисунок 7.2

Затем был добавлен аудит отказа для всех пользователей – рисунок 7.3.

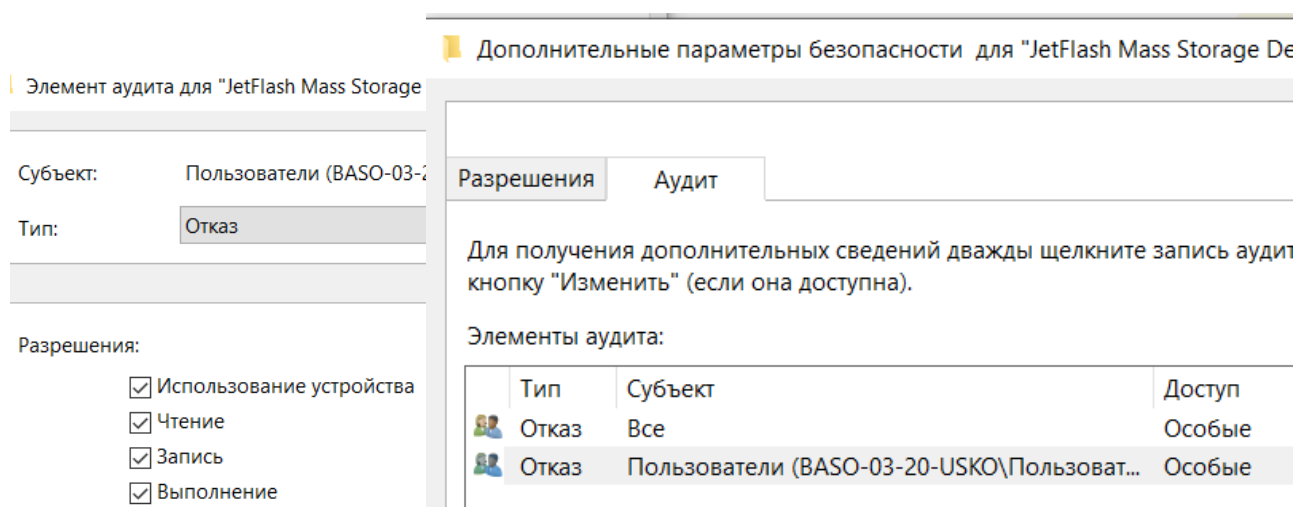


Рисунок 7.3

После был установлен запрет всем пользователям на использование незарегистрированных USB-флэш-накопителей (устройств хранения), с помощью параметров контроля – рисунок 7.4.

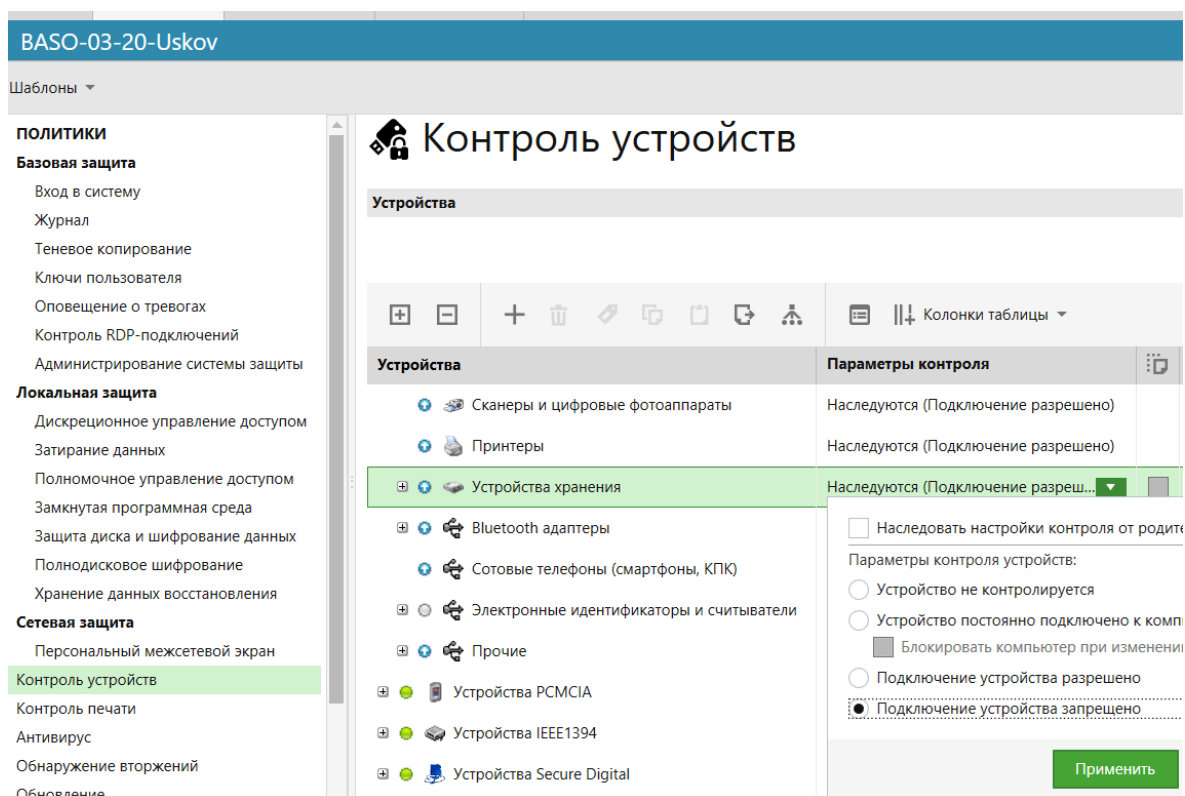


Рисунок 7.4

Для отслеживания произошедших событий, связанных с работой механизма разграничения доступа к устройствам, была выполнена настройка регистрации событий, рисунок 7.5.

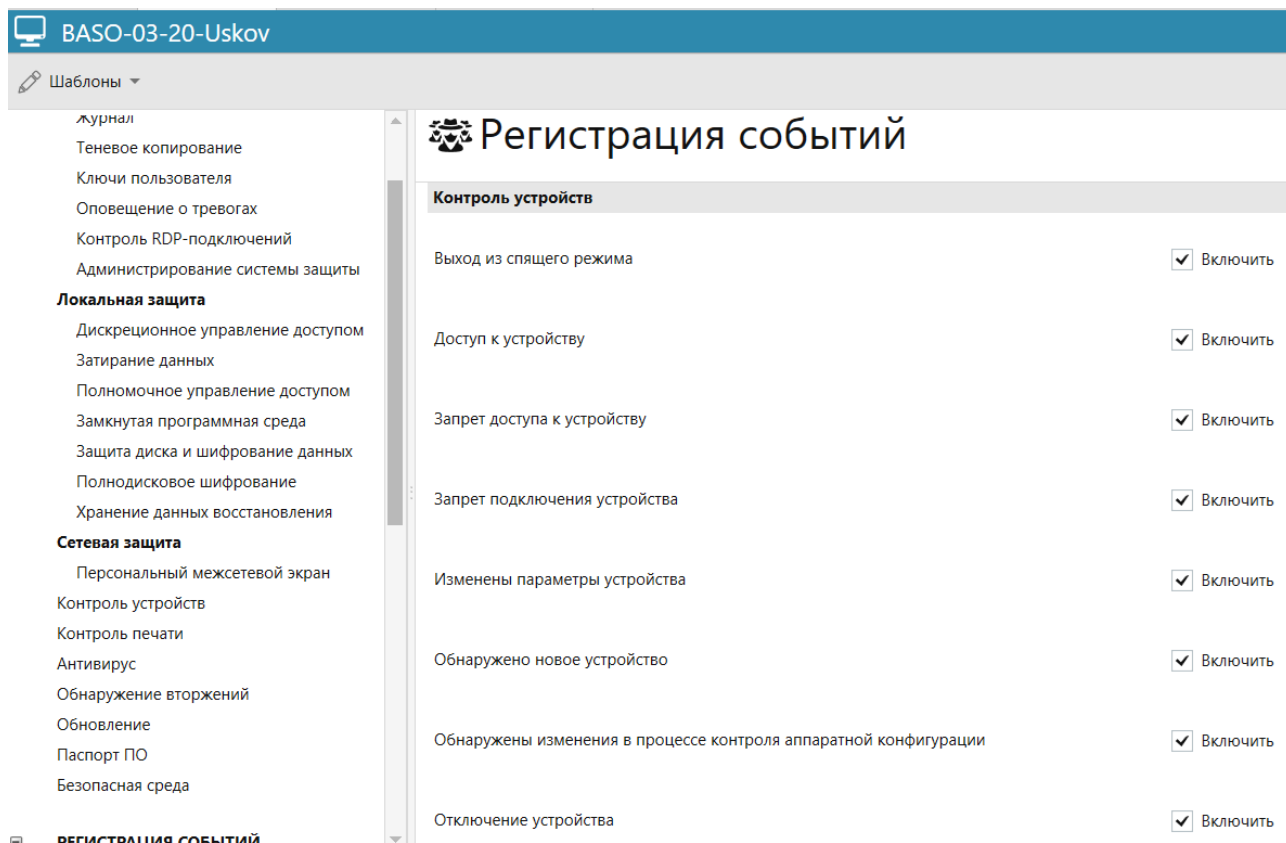


Рисунок 7.5

Авторизовавшись под уч. записью Uskov2 был замечен запрет на допуск к настроенному USB устройству, рисунок 7.6.

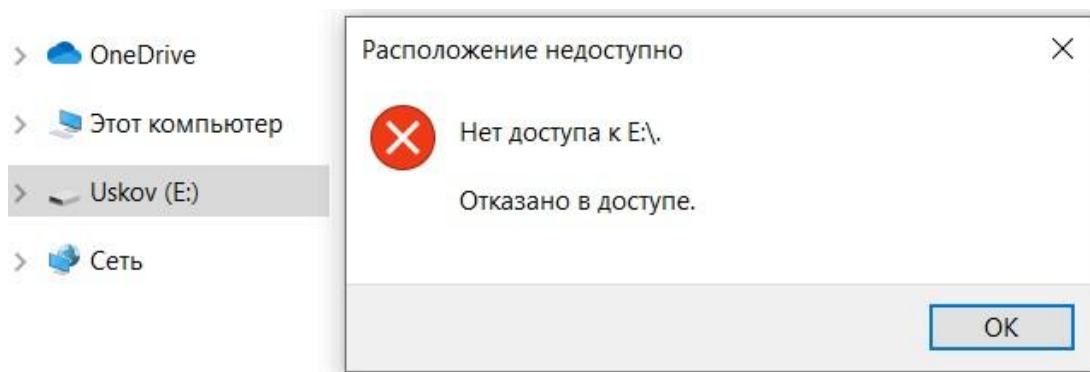


Рисунок 7.6

При этом от пользователя Uskov1 доступ к устройству был возможен, рисунок 7.7.

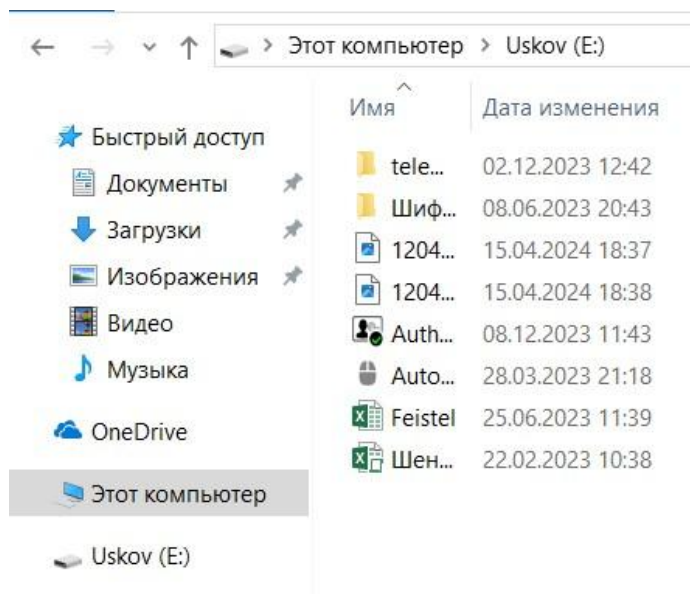


Рисунок 7.7

После проверки допуска к USB устройству была выполнена настройка разграничения доступа к устройству с помощью механизма полномочного управления доступом, т.е. присвоив ему требуемую категорию конфиденциальности. Для этого был отменен ранее установленный запрет с рисунка 7.2. А параметры допуска установлены в значение «Конфиденциально» – рисунок 7.8.

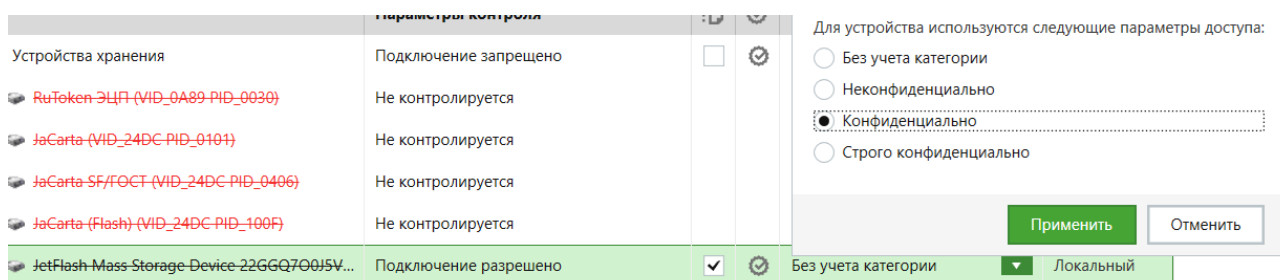


Рисунок 7.8

После применения настроек, попытка авторизации от пользователя Uskov2 закончилась ошибкой, поскольку его уровень допуска не соответствует уровню

допуска USB устройства – рисунок 7.9.

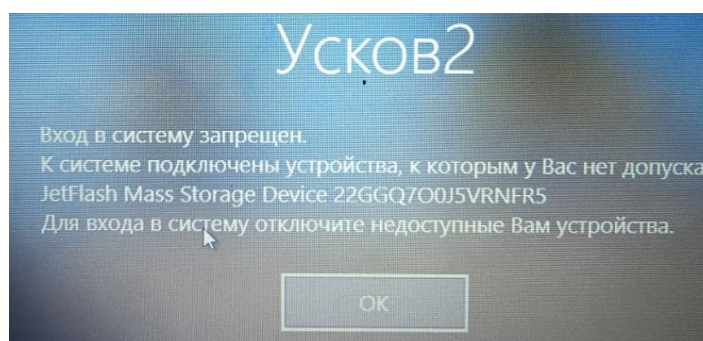


Рисунок 7.9

В случае если рассматриваемое USB устройство не подключено, то вход возможен. При успешной авторизации пользователя Uskov2 или др., подключение USB устройства в качестве устройства хранения не возможно, поскольку был настроен допуск только для 1 устройства. Ошибка подключения представлена на рисунке 7.10.

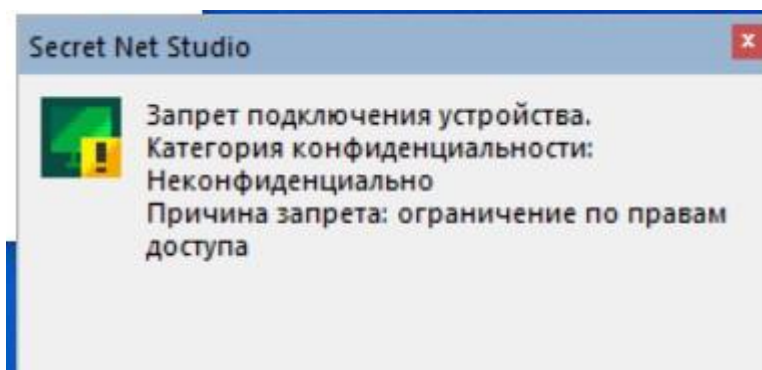


Рисунок 7.10

После был изучен журнал событий категории «Разграничение доступа к устройствам» и типом «Аудит отказов». Ошибка допуска показанная на рисунке 7.9 отображена в журнале на рисунке 7.11, а ошибка подключения незарегистрированного USB накопителя данных показанная на рисунке 7.10 отображена на рисунке 7.12.

	24.04.2024...	Запрет подключения устройства.	Разграниче...	BASO-03-20-Uskov	СИСТЕМА
--	---------------	--------------------------------	---------------	------------------	---------

ДЕТАЛЬНО	ОБЩЕЕ	ПАРАМЕТРЫ
-----------------	-------	-----------

Описание

Запрет подключения устройства.
 Категория конфиденциальности: Строго конфиденциально
 Причина запрета: ограничение по категории конфиденциальности

Устройство

JetFlash Mass Storage Device 22GGQ700J5VRNFR5

Группа:	Устройства USB
Класс:	Хранение данных
Описание:	Mass Storage Device
Производитель:	JetFlash
Серийный номер:	22GGQ700J5VRNFR5

Рисунок 7.11

	24.04.2024...	Запрет подключения устройства.	Разграниче...	BASO-03-20-Uskov
--	---------------	--------------------------------	---------------	------------------

ДЕТАЛЬНО	ОБЩЕЕ	ПАРАМЕТРЫ
-----------------	-------	-----------

Описание

Запрет подключения устройства.
 Категория конфиденциальности: Неконфиденциально
 Причина запрета: ограничение по правам доступа

Устройство

USB Flash Memory 0060E049DF72EDC1D000A040

Группа:	Устройства USB
Класс:	Хранение данных
Описание:	USB Flash Memory
Производитель:	
Серийный номер:	0060E049DF72EDC1D000A040

Рисунок 7.12

Управление доступом к подключаемым USB-флэш-накопителям было успешно выполнено.

8 ЗАДАНИЕ №8

Настройка механизма замкнутой программной среды на рабочем месте пользователя автоматизированной системы в защищенном исполнении.

Ход выполнения задания

Используя приложение SNS «Локальный центр управления», для пользователя korus было исключено действие правил замкнутой программной среды, несмотря на то, что он входит в группу администраторов, рисунок 8.1.

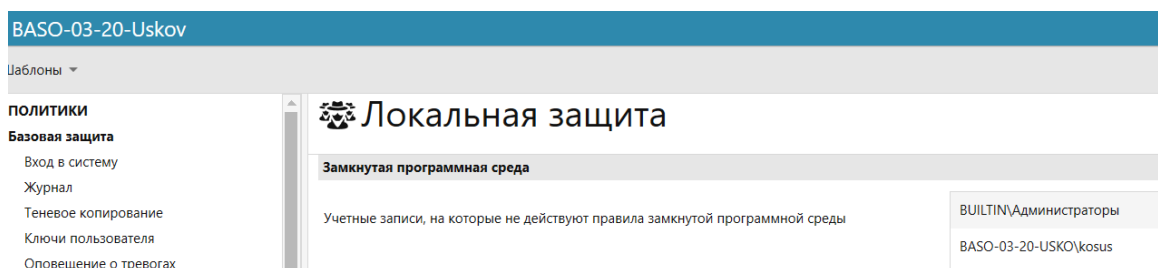


Рисунок 8.1

После были предприняты шаги по созданию новой модели данных для замкнутой программной среды. На экране отобразилось диалоговое окно «Настройка контроля по умолчанию» (Default control settings), рисунок 8.2. Был добавлен пункт предварительной очистки модели данных.

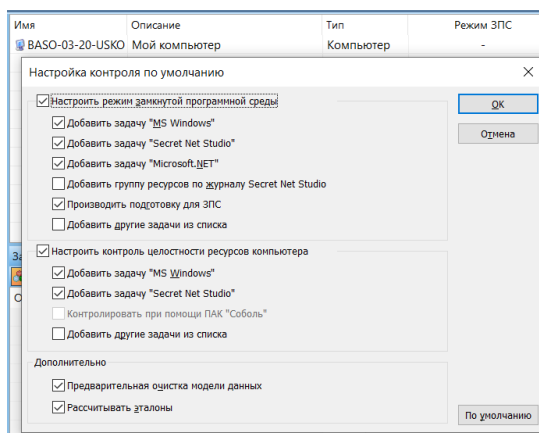


Рисунок 8.2

Программа запустила поиск установленных программ и добавление задач, затем была подготовка ресурсов для использования в ЗПС и наконец выполнен расчёт эталонов для ресурсов, рисунок 8.3.

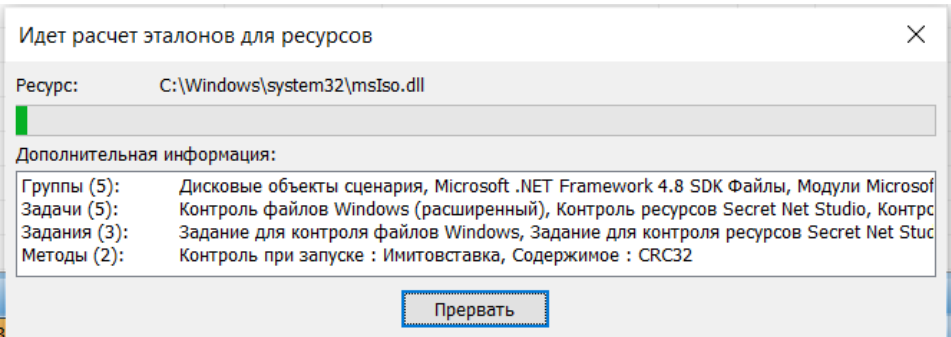


Рисунок 8.3

Было создано новое задания на ЗПС, рисунок 8.4.

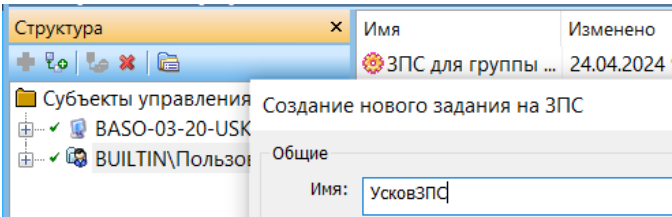


Рисунок 8.4

Затем был включен мягкий режим ЗПС для субъекта управления «BASO-03-20-USKOV», рисунок 8.5.

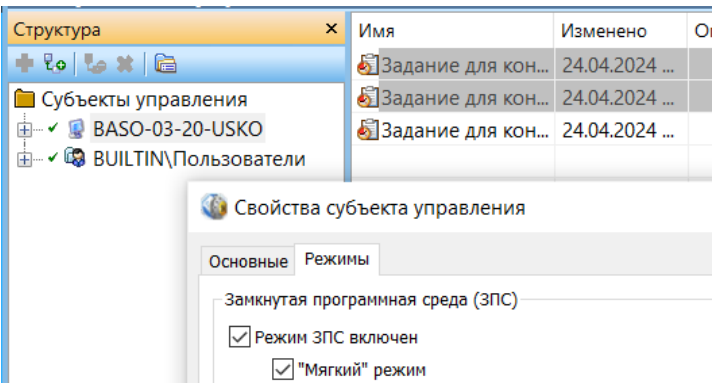


Рисунок 8.5

Под учётной записью администратора был открыт журнал Secret Net Studio и выполнен его экспорт во внешний файл с удалением после экспорта, рисунок 8.6.

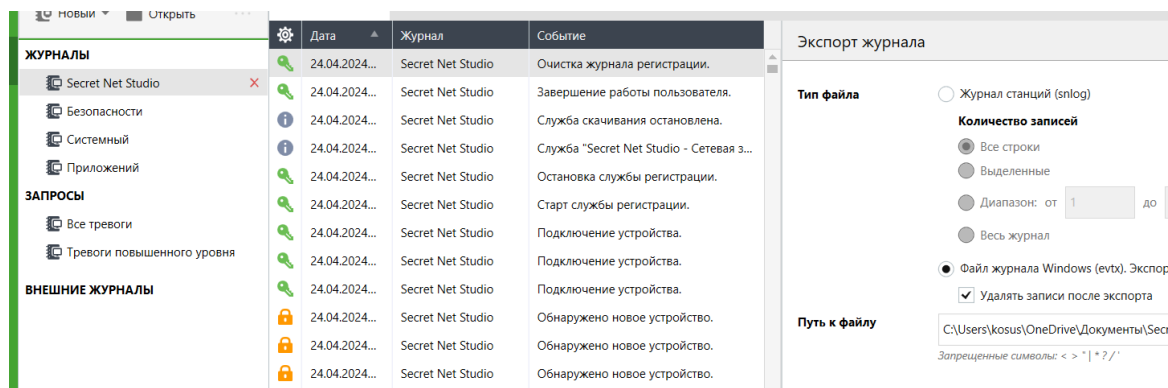


Рисунок 8.6

Затем был перезапущен компьютер и выполнен вход в систему под учетной записью «Uskov1», запущены все программы, которые должны быть разрешены пользователю. Сеанс был завершён, а после выполнен вход в систему под учетной записью администратора. Для созданного ранее задания была добавлена новая группа по журналу, рисунок 8.7.

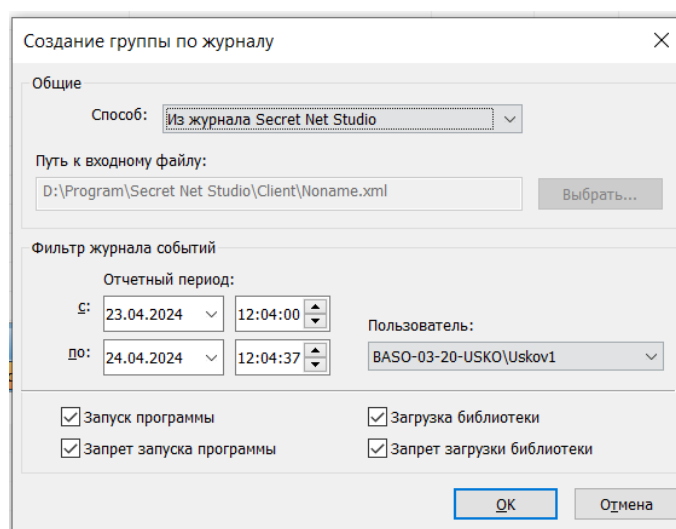


Рисунок 8.7

После добавления группы был отключён мягкий режим ЗПС и сохранена

созданная ранее модель данных.

Под учетной записью пользователя «Uskov1» была возможность запускать только ограниченный набор программ: Проводник, LibreOffice Writer, Paint 3D, Календарь, Корзина.

При попытке запустить другие программы отображались ошибки, рисунок 8.8.

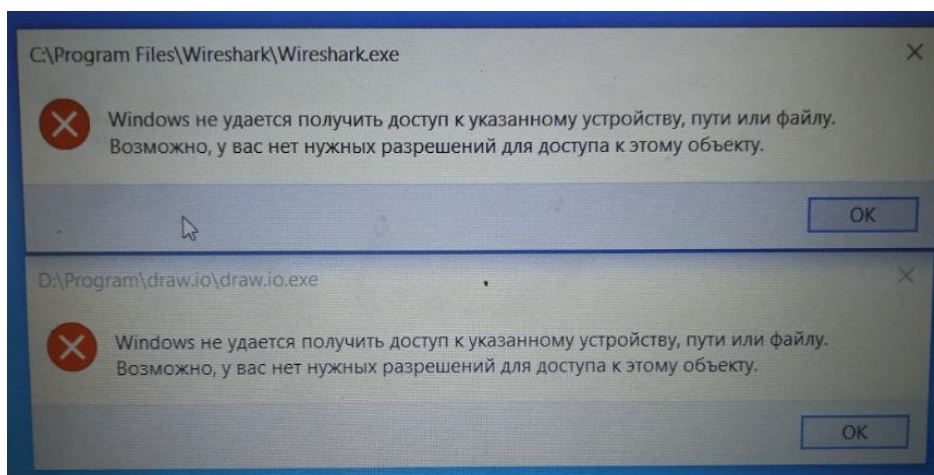


Рисунок 8.8

Для пользователя Uskov2 также был возможен запуск приложения из разрешённого перечня, а запуск других приложений не начинался – отображалась ошибка, рисунок 8.9.

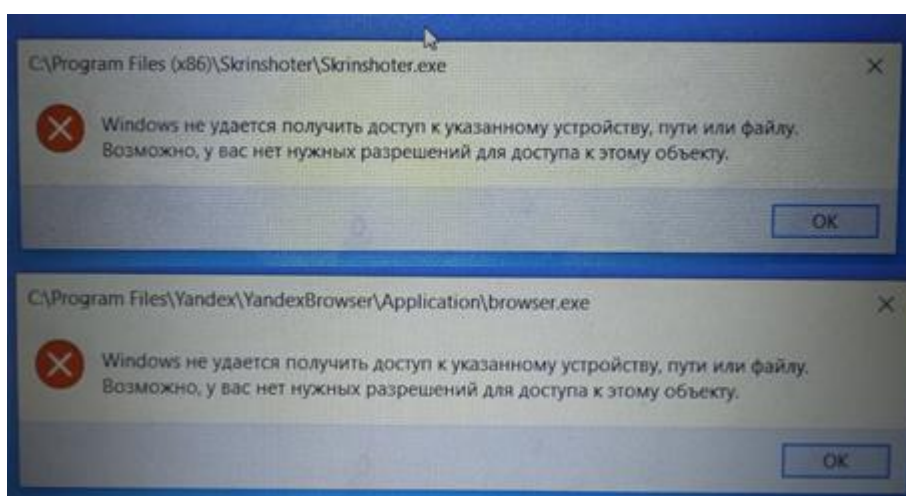


Рисунок 8.9

Войдя в систему под учетной записью администратора и открыв журнал Secret Net Studio, было выполнено ознакомление с записями журнала, имеющими категорию «Замкнутая программная среда». На рисунке 8.10 можно заметить отказ в запуске приложения Skrinshoter.

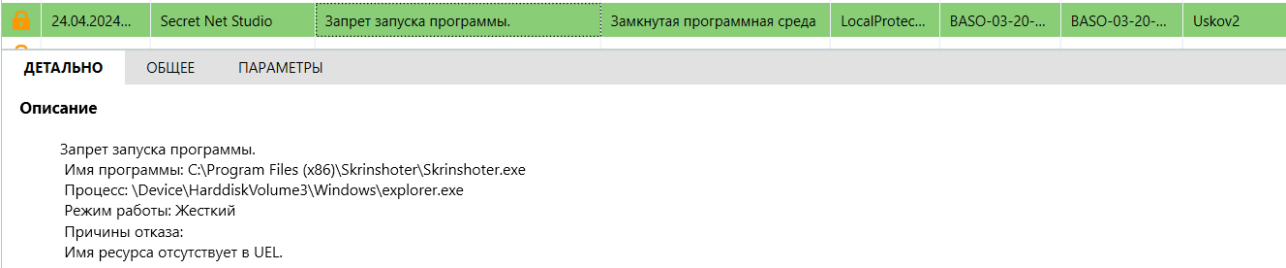


Рисунок 8.10

После успешной настройки ЗПС для пользователей АРМ и ознакомления с журналом, данная функция была отключена.

9 ЗАДАНИЕ №9

Настройка механизма контроля целостности ресурсов на рабочем месте пользователя автоматизированной системы в защищенном исполнении.

Ход выполнения задания

На диске «С» была создана папка «Контроль целостности», в которой создан файл, названный «УсковКЦ», и внесена в него произвольная информация, рисунок 9.1.

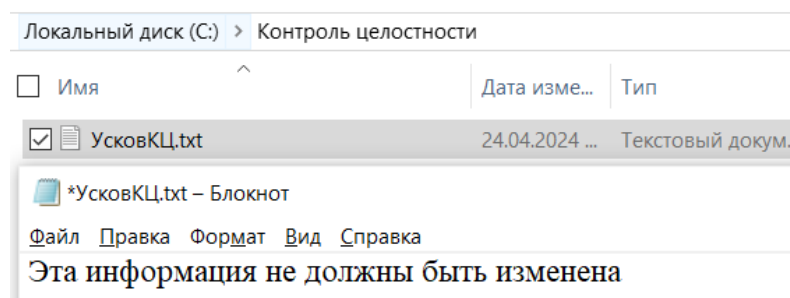


Рисунок 9.1

Затем был создан новый ресурс Windows для КЦ, рисунок 9.2.

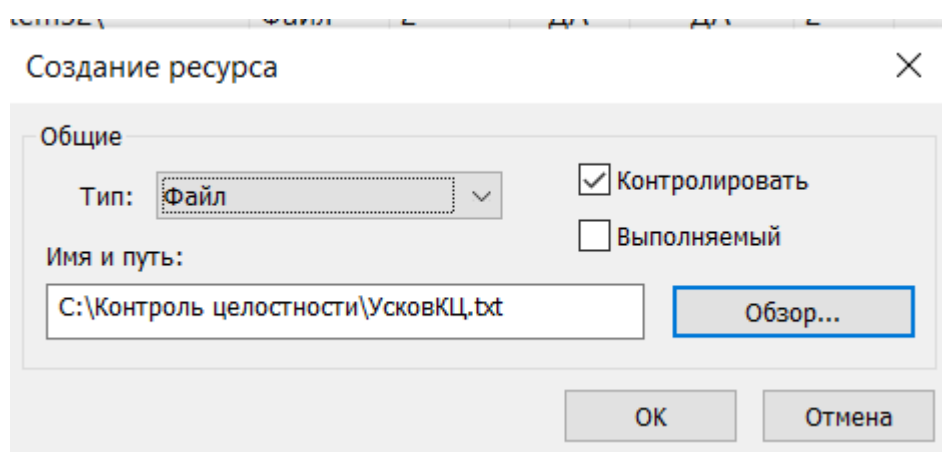


Рисунок 9.2

После была создана группа ресурсов, рисунок 9.3.

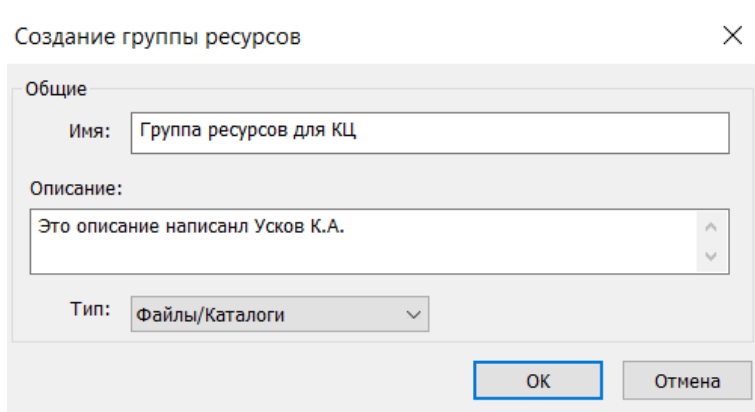


Рисунок 9.3

В группу ресурсов был добавлен созданный ранее ресурс, рисунок 9.4.

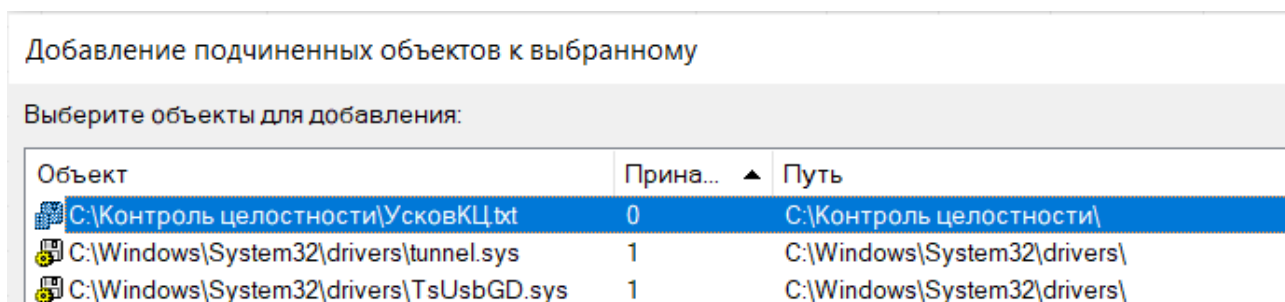


Рисунок 9.4

Затем было создано задание «КЦ в документе» и в неё добавлена созданная ранее группа. Было создано новое задание для КЦ, рисунок 9.5.

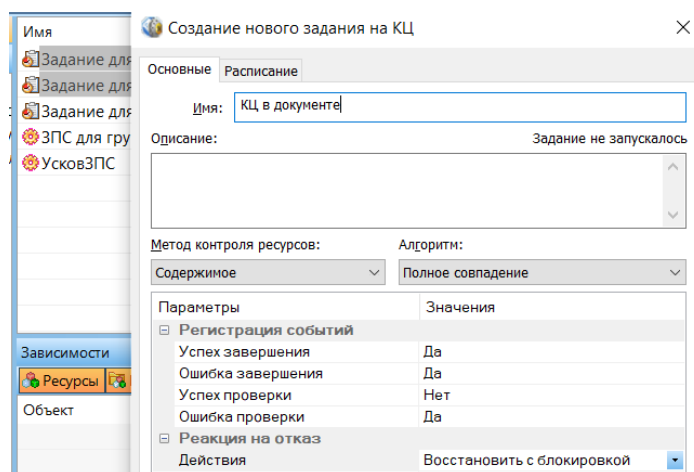


Рисунок 9.5

Во вкладке «Расписание» было установлено «При загрузке ОС». В созданное задание «КЦ в документе» была добавлена задача «КЦ в документе». Для компьютера было добавлено задание из существующих – «КЦ в документе», рисунок 9.6.

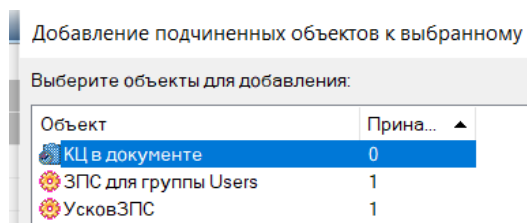


Рисунок 9.6

После добавления задания, был выполнен расчёт эталонов, рисунок 9.7.

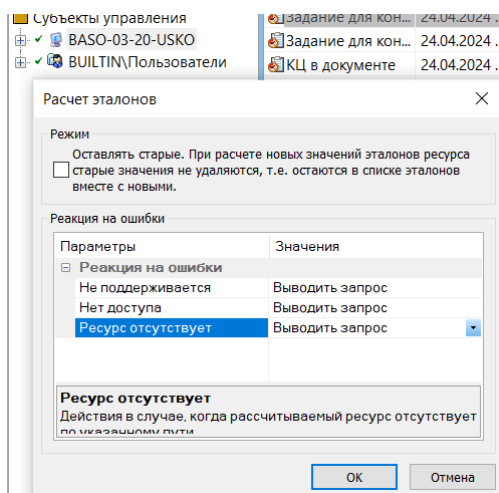


Рисунок 9.7

После завершения расчета эталонов, новая модель данных была сохранена, а компьютер перезагружен. Под учётной записью Uskov1 созданный текстовый файл, на который распространяется контроль целостности, был изменён. И после перезагрузки компьютера, вход от пользователя Uskov1 был уже невозможен. Авторизовавшийся в системе под учётной записью администратора, было предложено разблокировать компьютер. Два последних события отображены на рисунке 9.8.

ВЫВОД

В ходе выполнения практических заданий был успешно выполнены поставленные задачи:

1) Установка автономного варианта SNS на рабочем месте пользователя автоматизированной системы в защищенном исполнении.

2) Настройка политик безопасности для SNS, установленного на рабочем месте пользователя автоматизированной системы в защищенном исполнении.

3) Настройка в SNS полномочного управления доступом к ресурсам рабочего места пользователя автоматизированной системы в защищенном исполнении.

4) Настройка аудита операционной системы рабочего места автоматизированной системы и событий SNS.

5) Работа с журналом событий SNS, установленного на рабочем месте пользователя автоматизированной системы.

6) Настройка механизма дискреционного управления доступом к файлам рабочего места пользователя автоматизированной системы в защищенном исполнении.

7) Управление доступом к подключаемым USB-флеш-накопителям на рабочем месте пользователя автоматизированной системы в защищенном исполнении.

8) Настройка механизма замкнутой программной среды на рабочем месте пользователя автоматизированной системы в защищенном исполнении.

9) Настройка механизма контроля целостности ресурсов на рабочем месте пользователя автоматизированной системы в защищенном исполнении.