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 № 17
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 № 17

Тема: устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем.

Цель: изучить механизмы устранения отказов и восстановления работоспособности компонентов систем защиты информации автоматизированных систем.

Ход работы:

Задание 1.

Результат выполнения работы представлен на рис.1 где мы установили 2 Windows server один из них AD а другой SNS. После установки отключили брандмауэр и настроили ip.

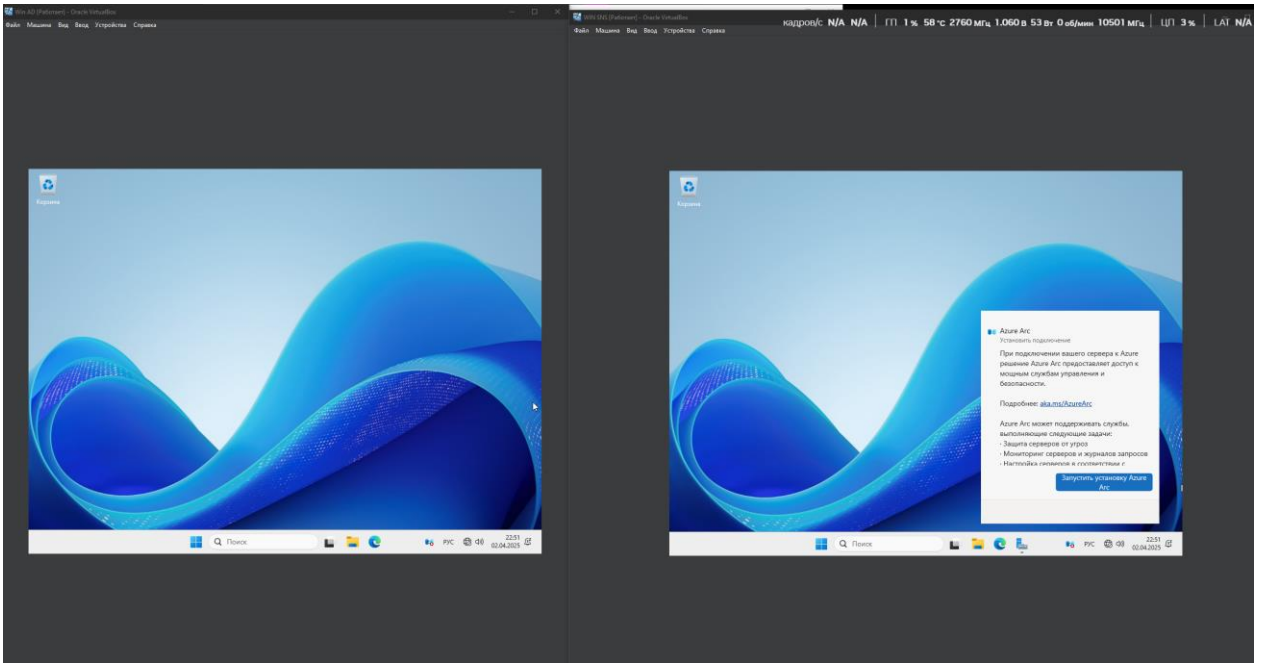

Рис. 1 Результат установки Win server 2025

Задание 2.

Установка необходимых компонентов для Доменные службы Active Directory и DNS-сервера представлен на рис. 2.

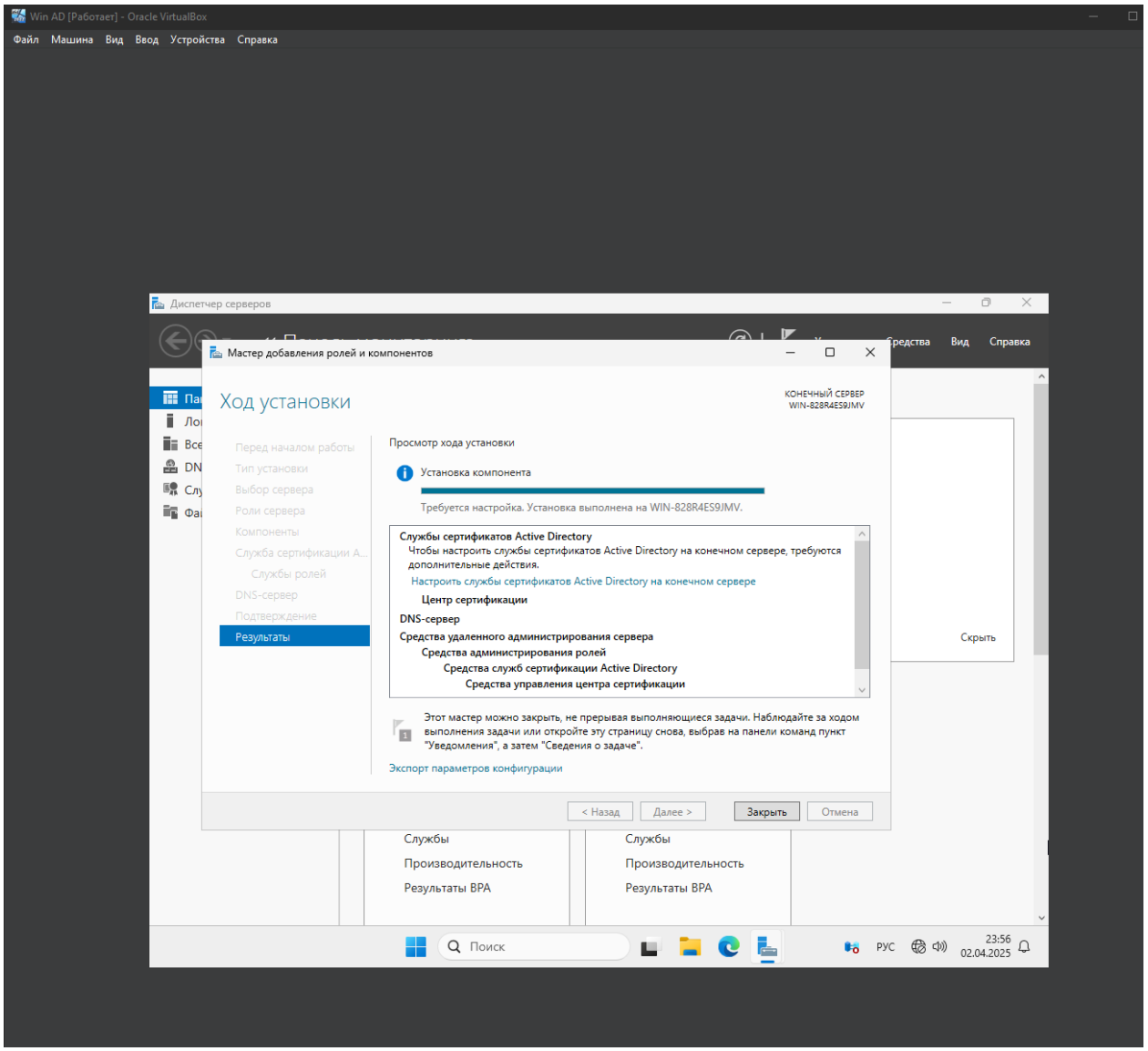

Рис. 2 установка компонентов

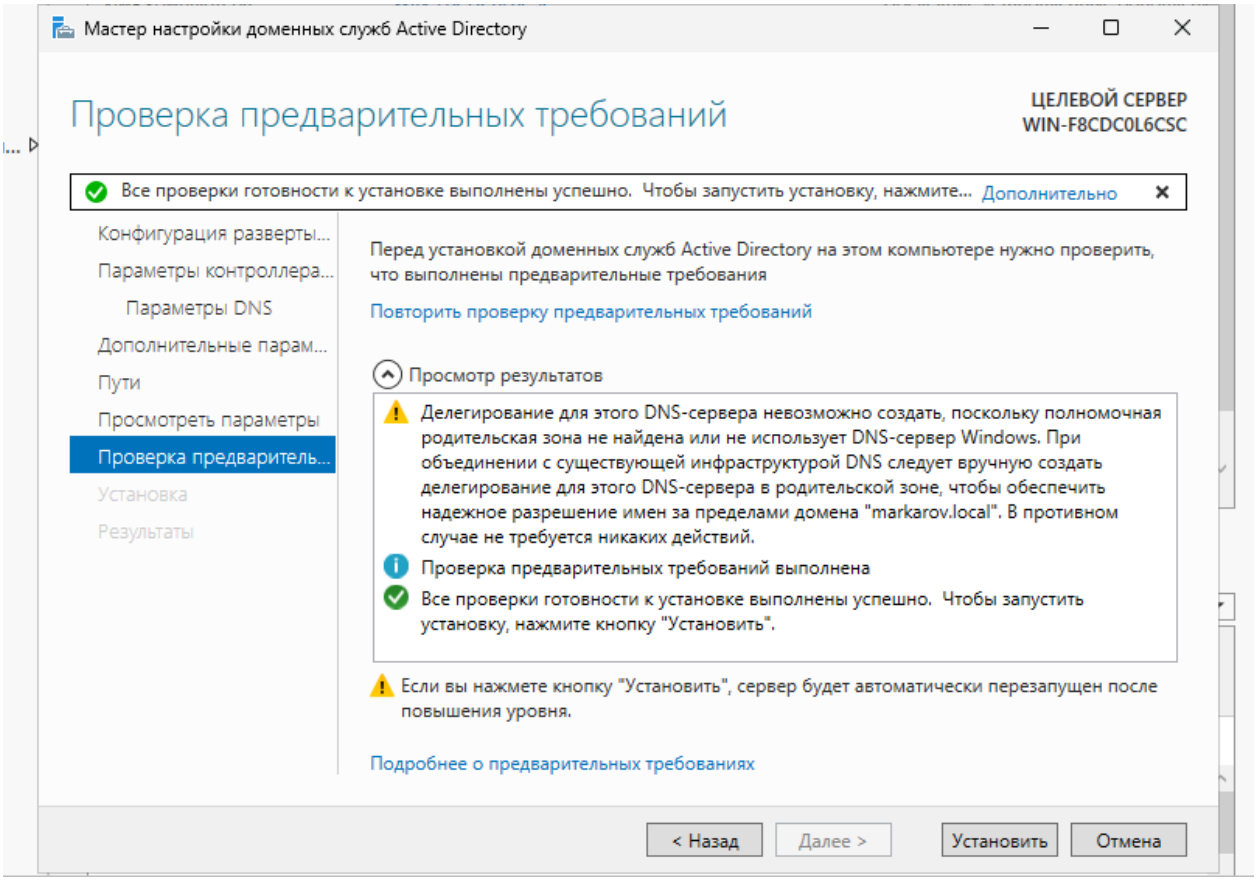

Рис. 3 проверка предварительных требований

Задание 3.

Через мастер настройки доменных служб Active Directory 3 добавить новый лес и указать имя корневого домена то что представленно на рис.3.

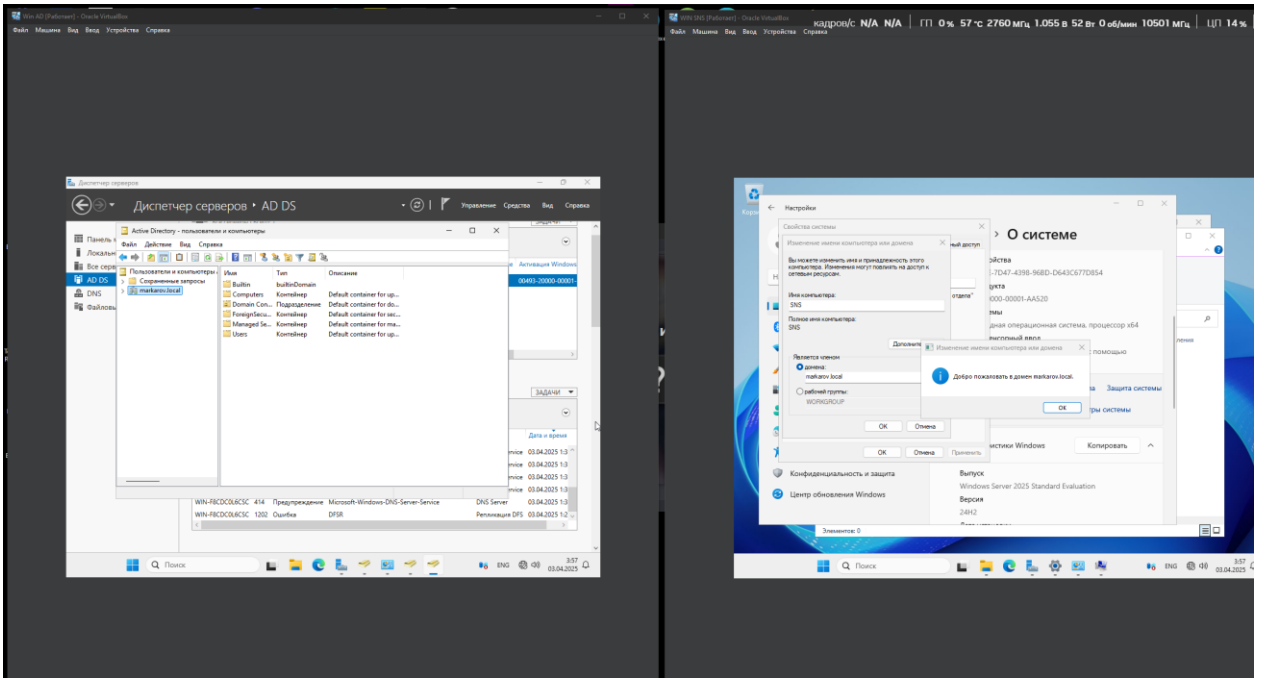

Рис. 4 Диспетчер серверов и установленный справа SN

Задание 4.

Ввести все виртуальные машины в созданный домен как показанно на рис.6.

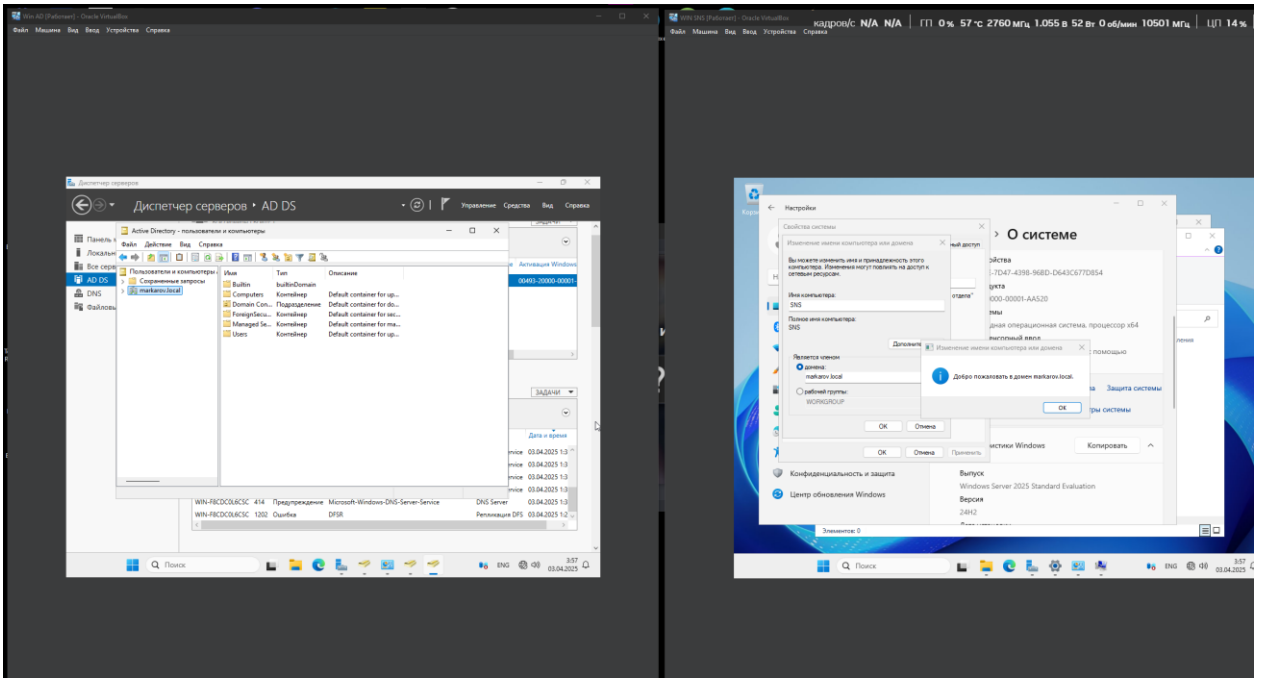

Рис. 5 процесс доабвления в домен компьютеры

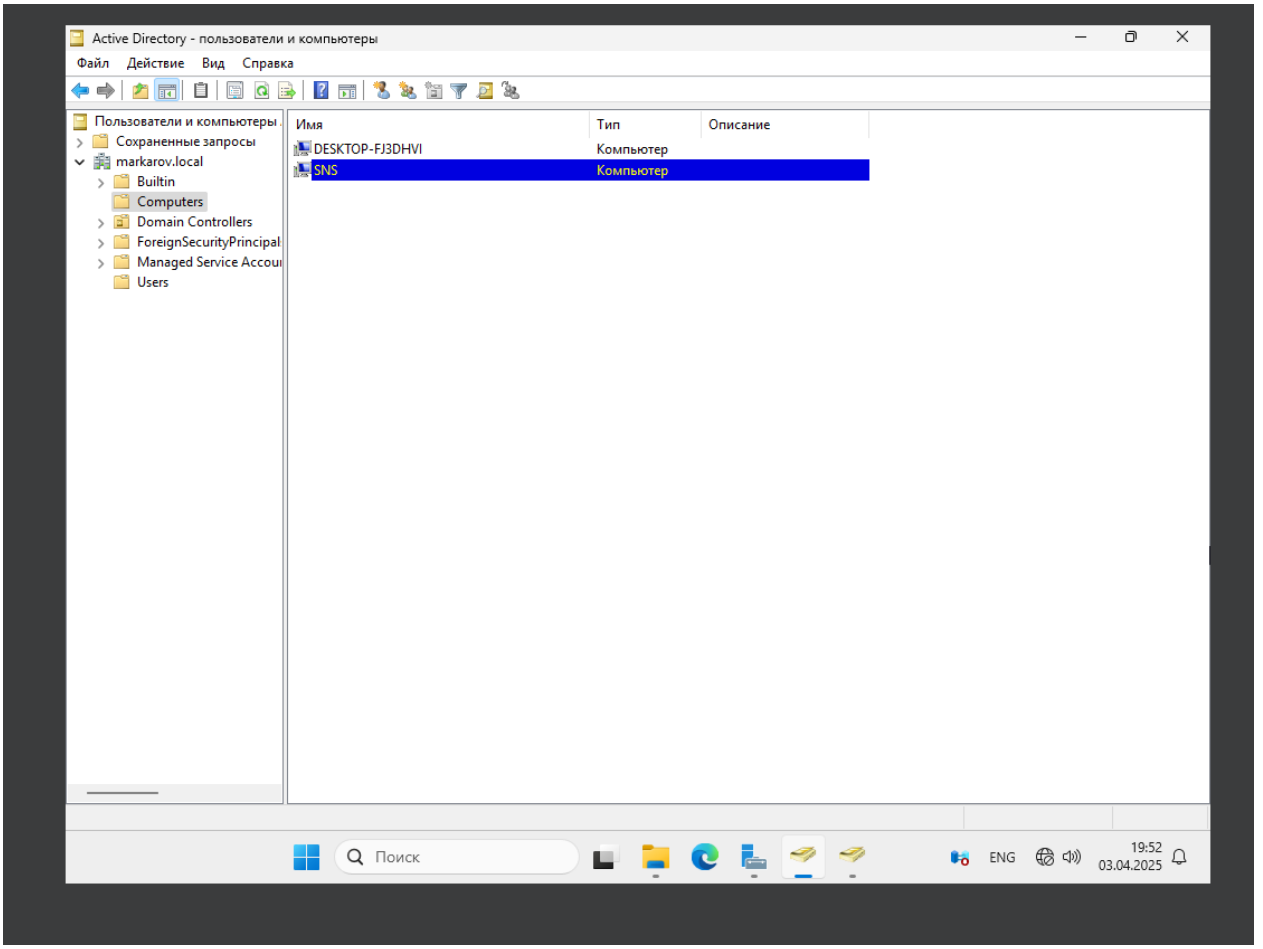

Рис. 6 конечный результат добавления виртуальных машины в домен

Задание 5.

Для дальнейшей работы Secret Net Studio в Active Directory необходимо

создать доменного пользователя «admin-sec» и две группы пользователей «sns-domain» и «sns-forest» после чего добавить в них admin-sec и на всех виртуальных машинах добавить этого пользователя в администраторы как показано на рис. 7.

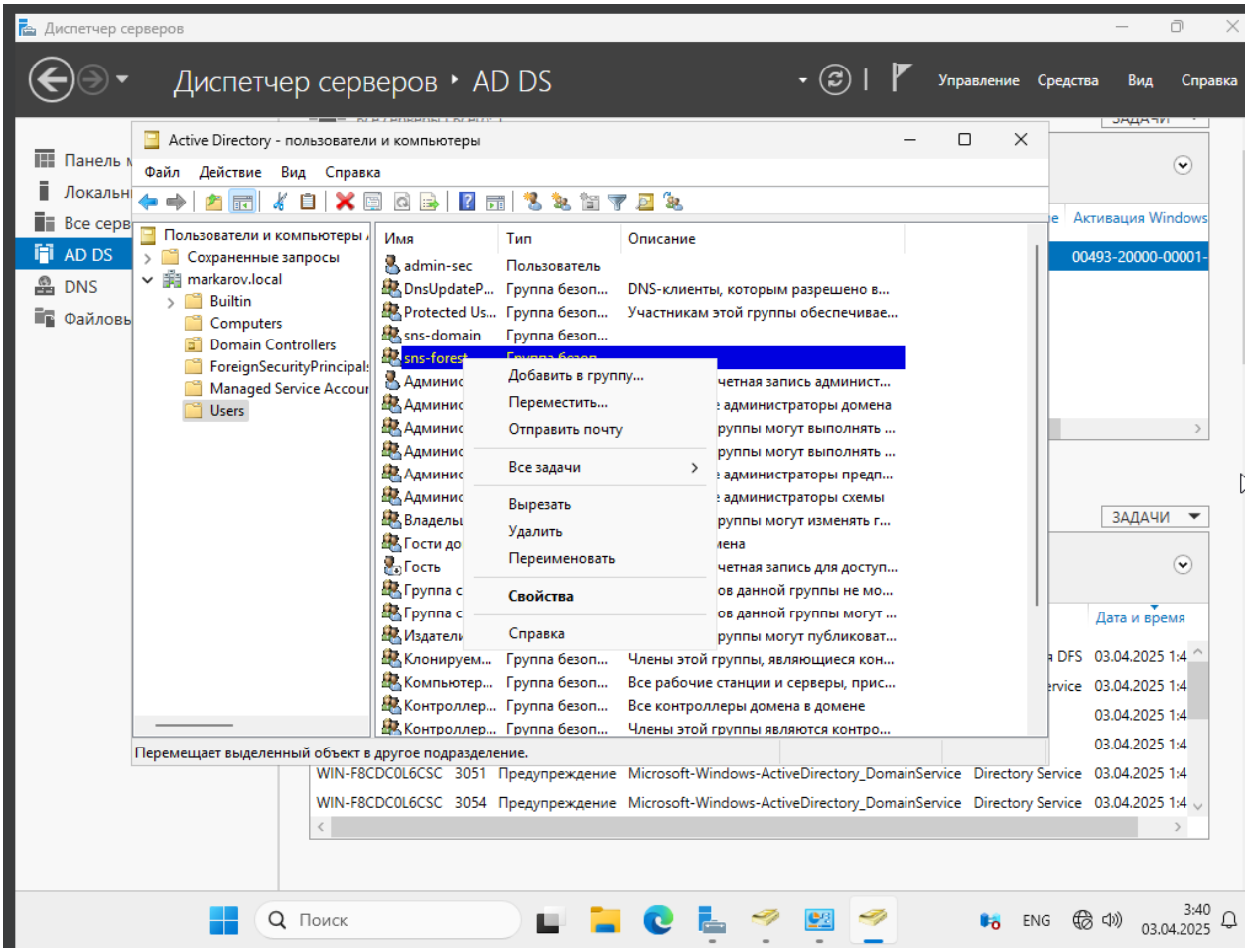

Рис. 7 процесс создание групп и пользователя домена

Задание 6.

На виртуальной машине Server-SNS установить функцию «.NET Framework 3.5» как показано на рис.8.

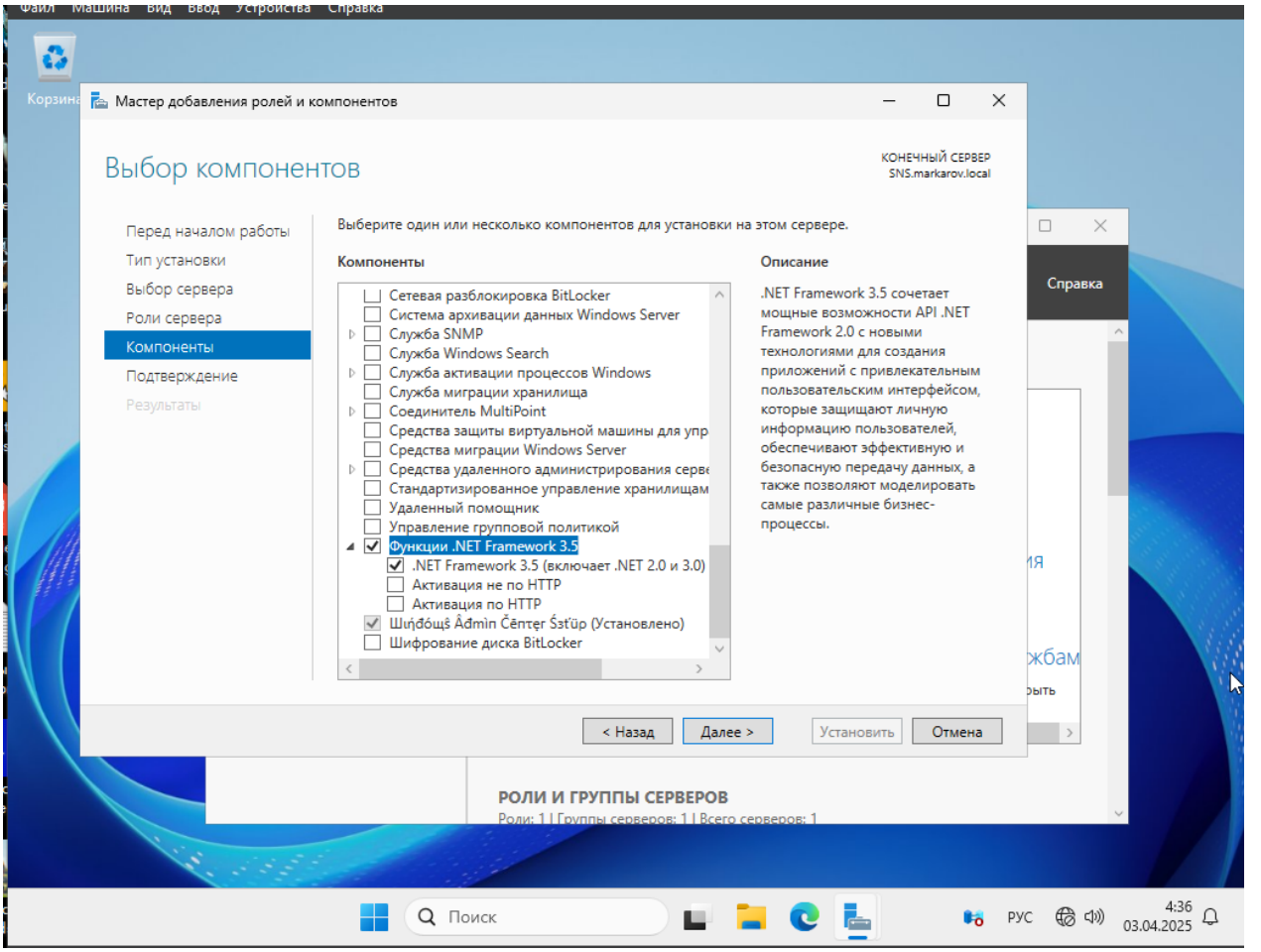

Рис. 8 Мастер добавления ролей и компонентов

Задание 7.

На виртуальной машине SNS выполним в ход в учётную запись admin-sec как представлено на рис.9.

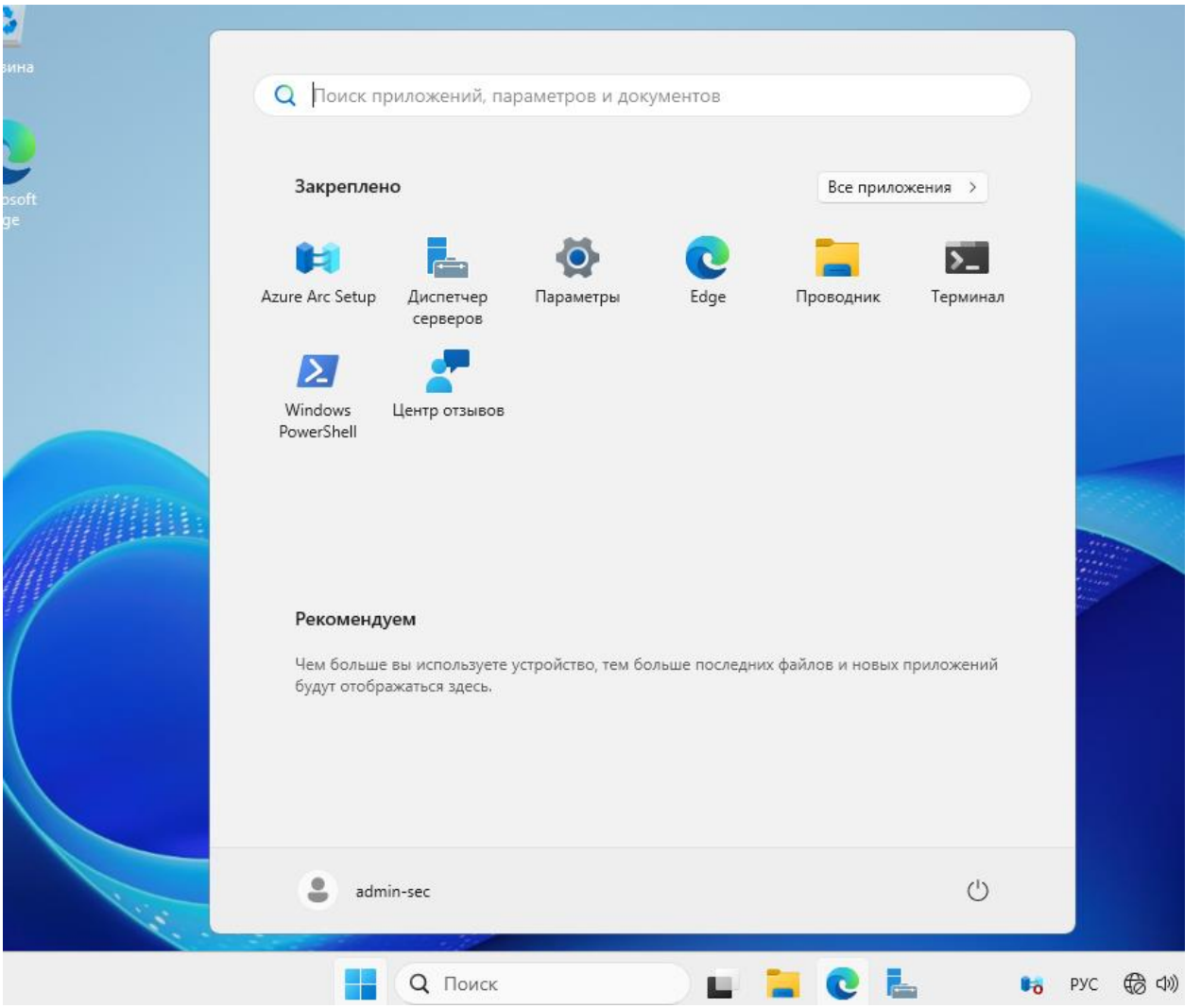

Рис. 9 пользователь SNS admin-sec

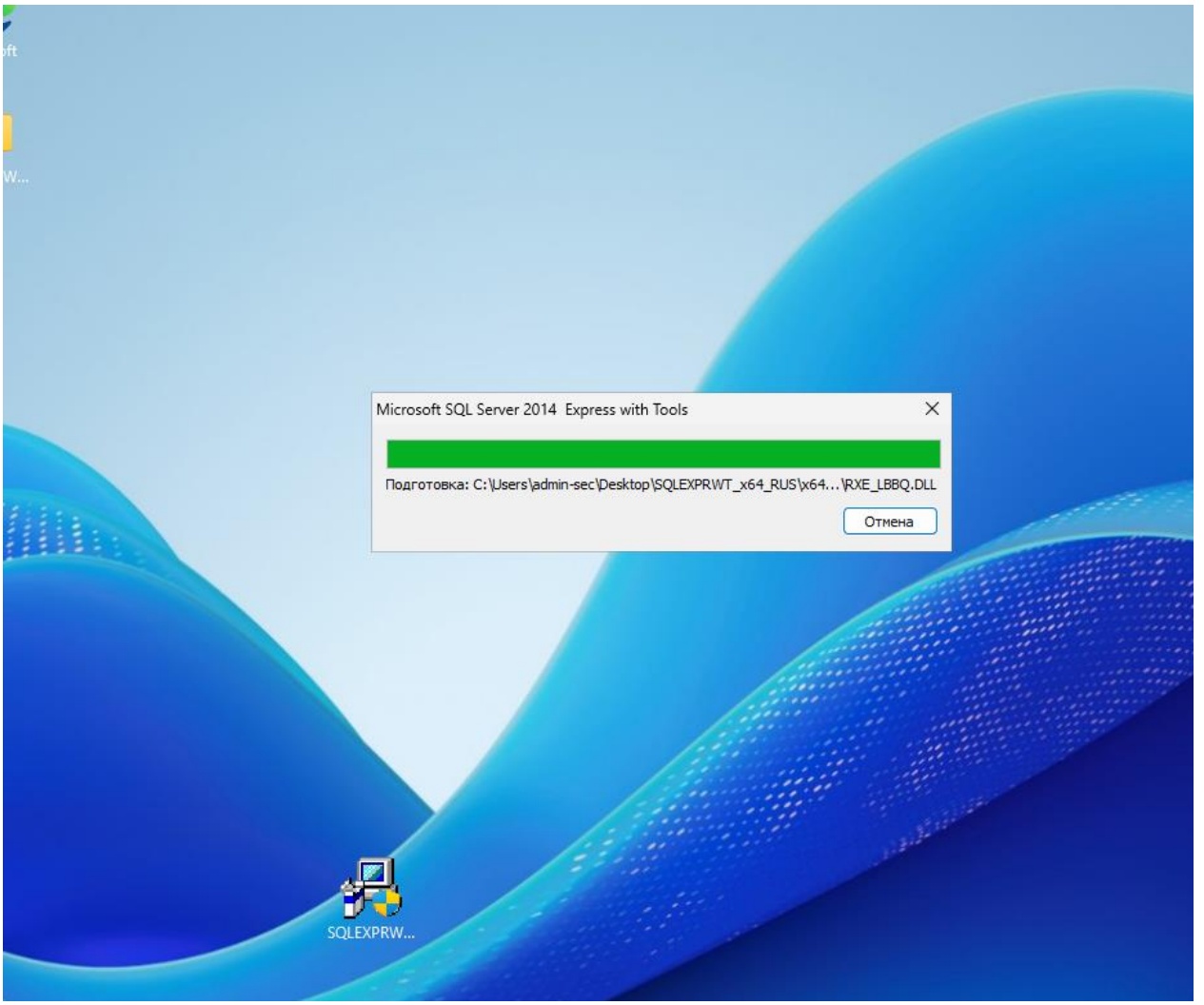

Рис. 10 процесс установления sql server 2014

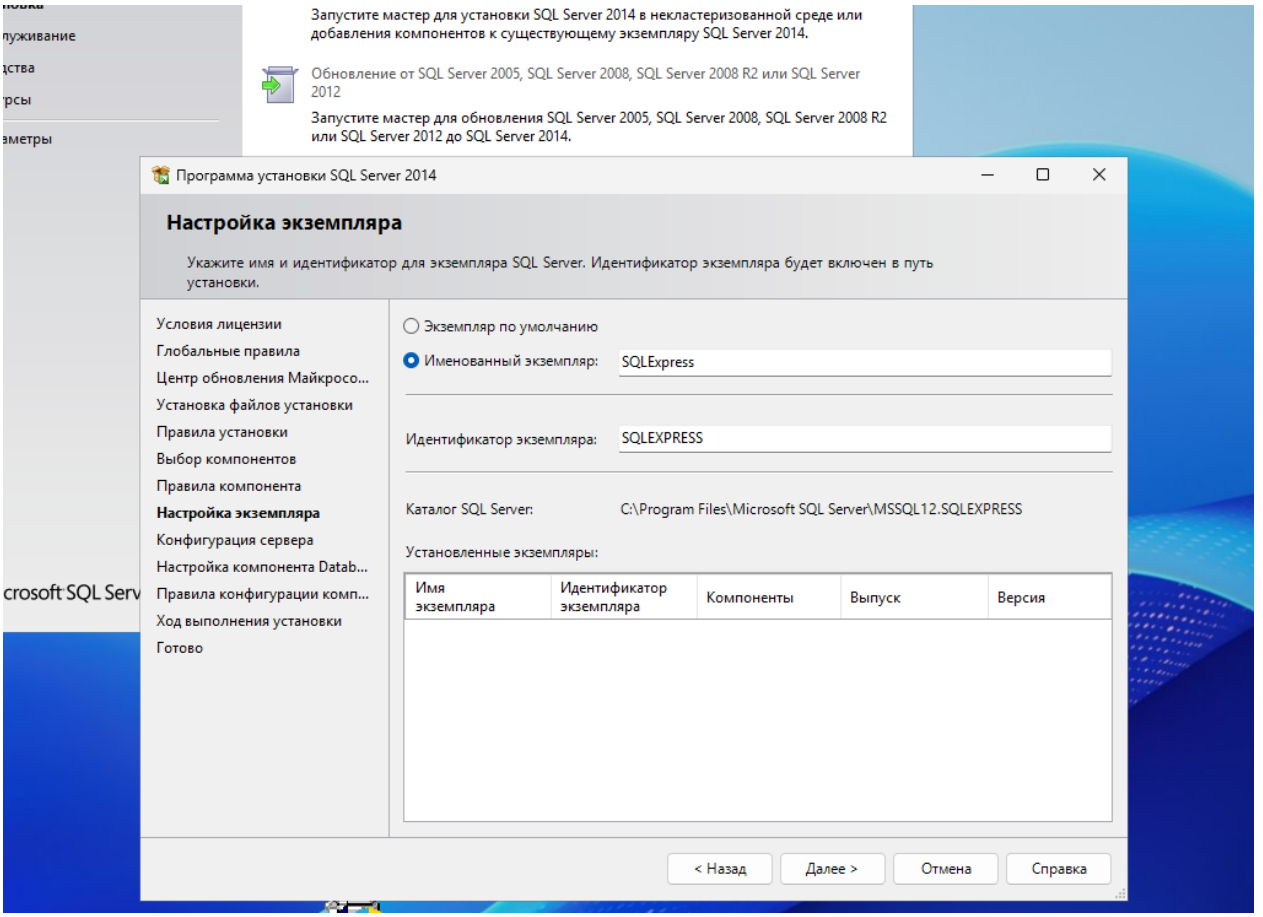

Рис. 11 процесс установки экземляляра

Задание 8.

Выключаем UAC защиту ставим нуль зашиту и перезагружаем виртуальную машину.

Задание 9.

Скачиваем папку и ключ лицензии Secret Net Studio 8.9 как показанно на рис. 12.

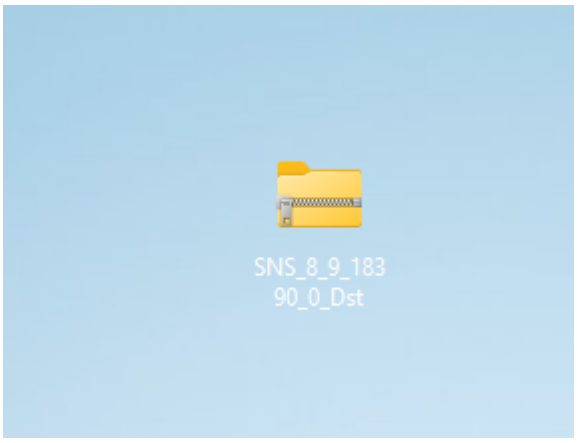

Рис. 12 файл для запуска SnAutoRun.exe

Задание 10.

На рис. 13 представлен процесс входа при котором мы использовали ранее созданный sql server и пароль для sa.

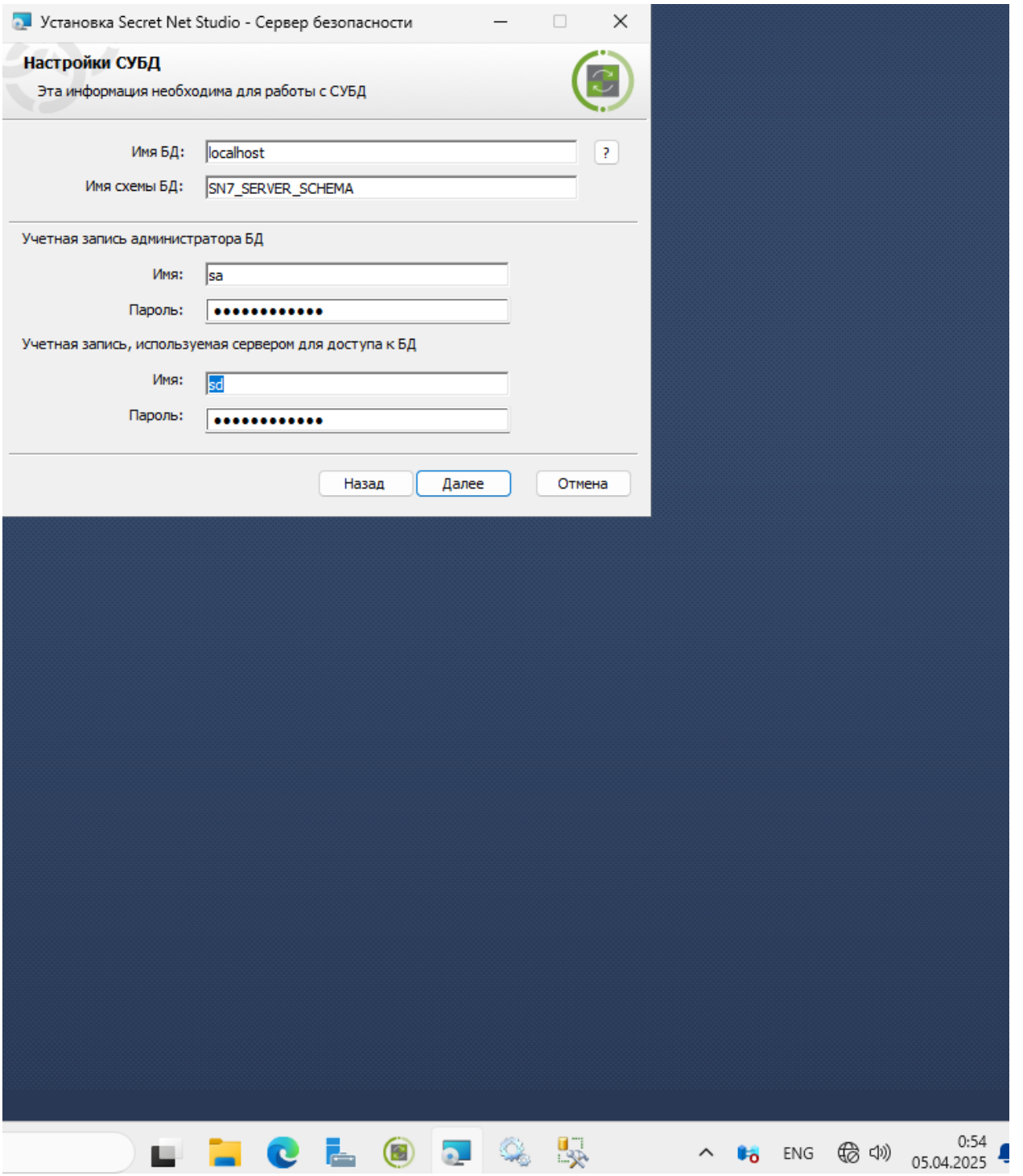

Рис. 13 вход в SECRET NET STUDIO

Вписываем название организации как показанно на рис. 14.

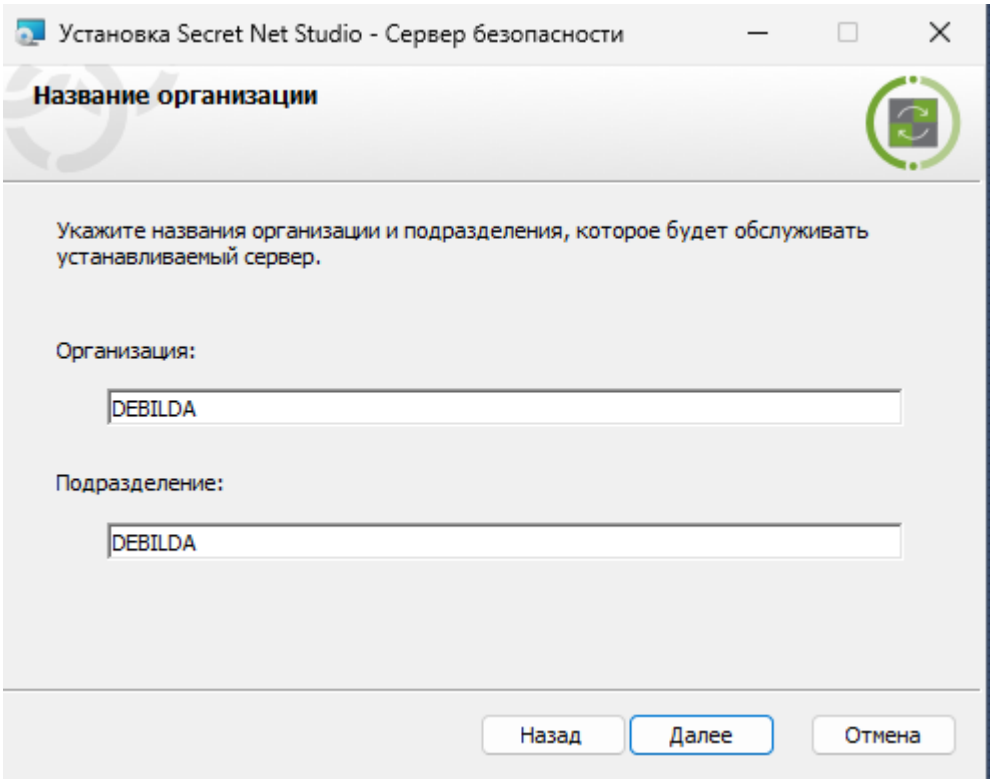

Рис. 14 наименование организации

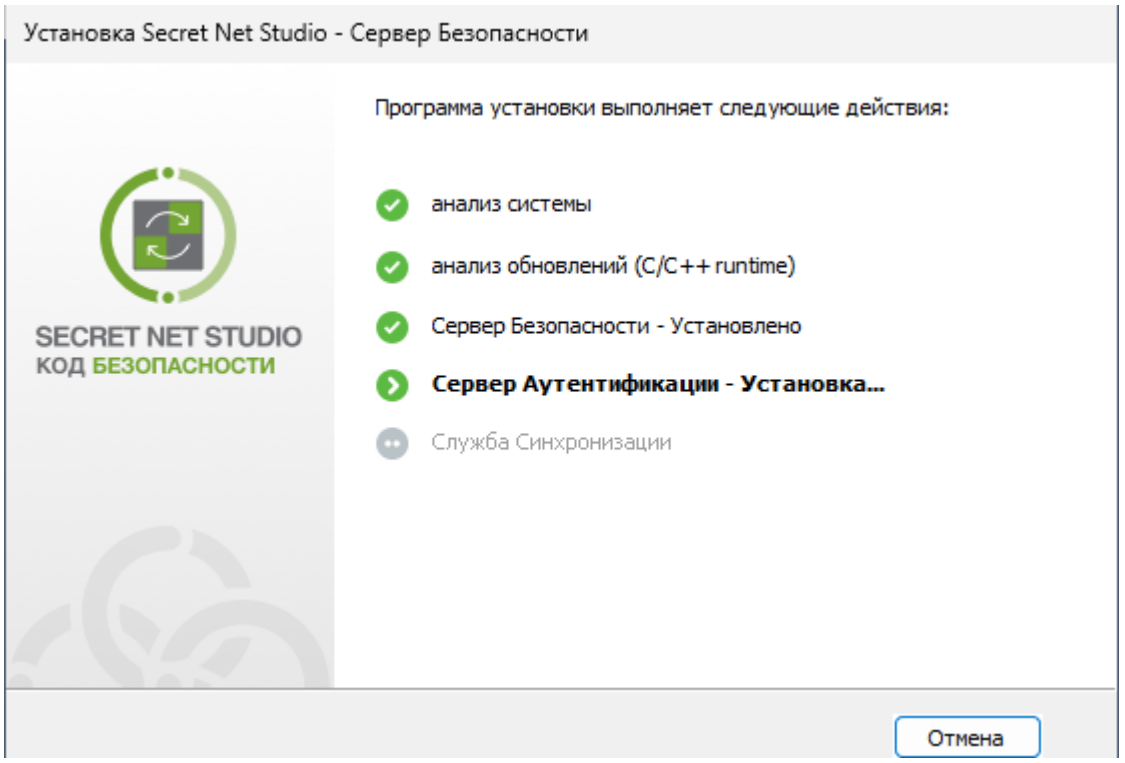

Рис. 15 результат установки

Задание 11.

Выполнить вход в доменную учетную запись «admin-sec», запустить установщик «SnAutoRun» и выбрать «Центр управления». Выполнить установку «Центра безопасности» как показанно на рис.16.

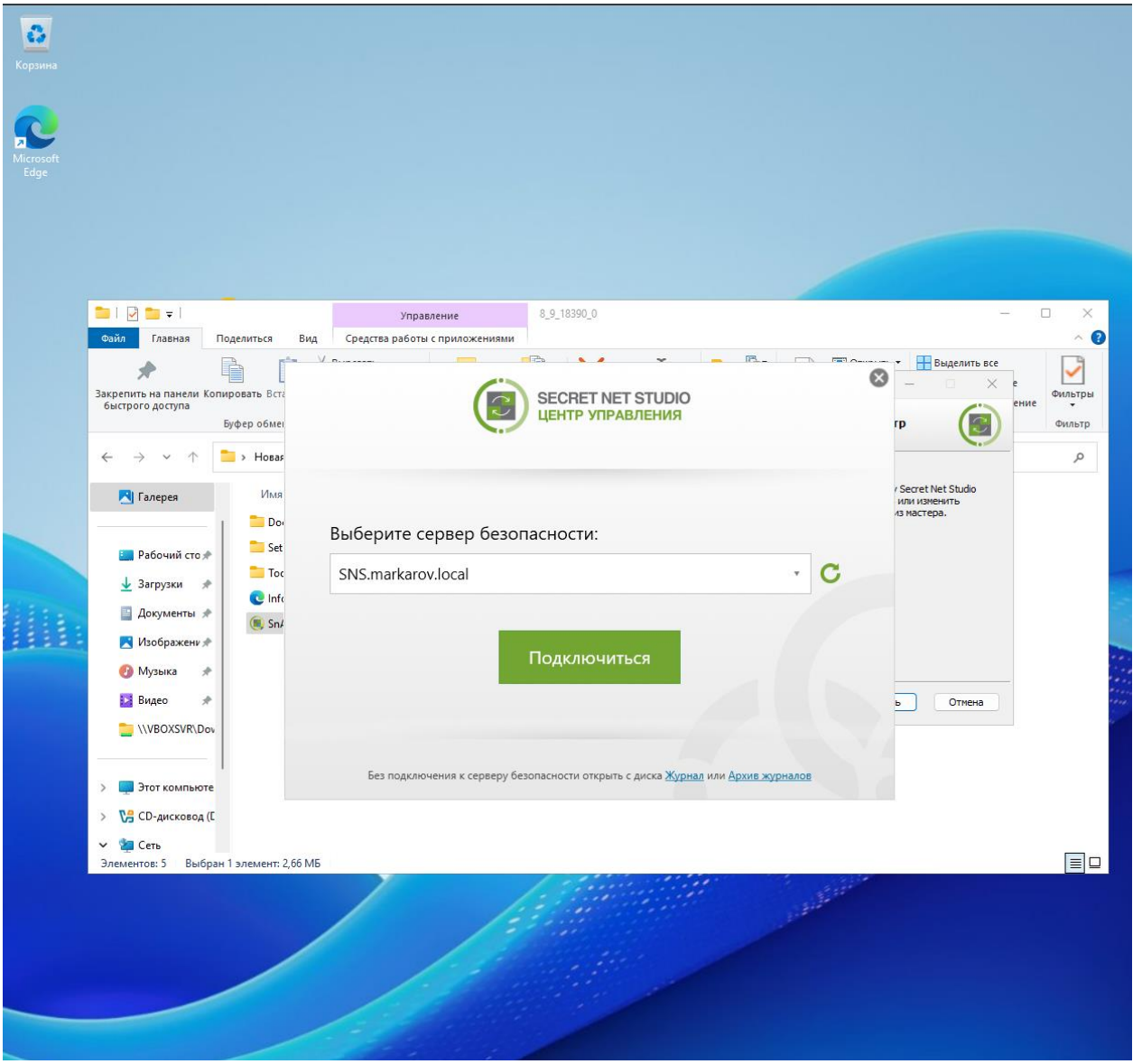

Рис. 16 вход в домен.

Задание 12.

Добавление папки дистрибутивов представлен на рис. 17. А окончательный результат на рис. 18.

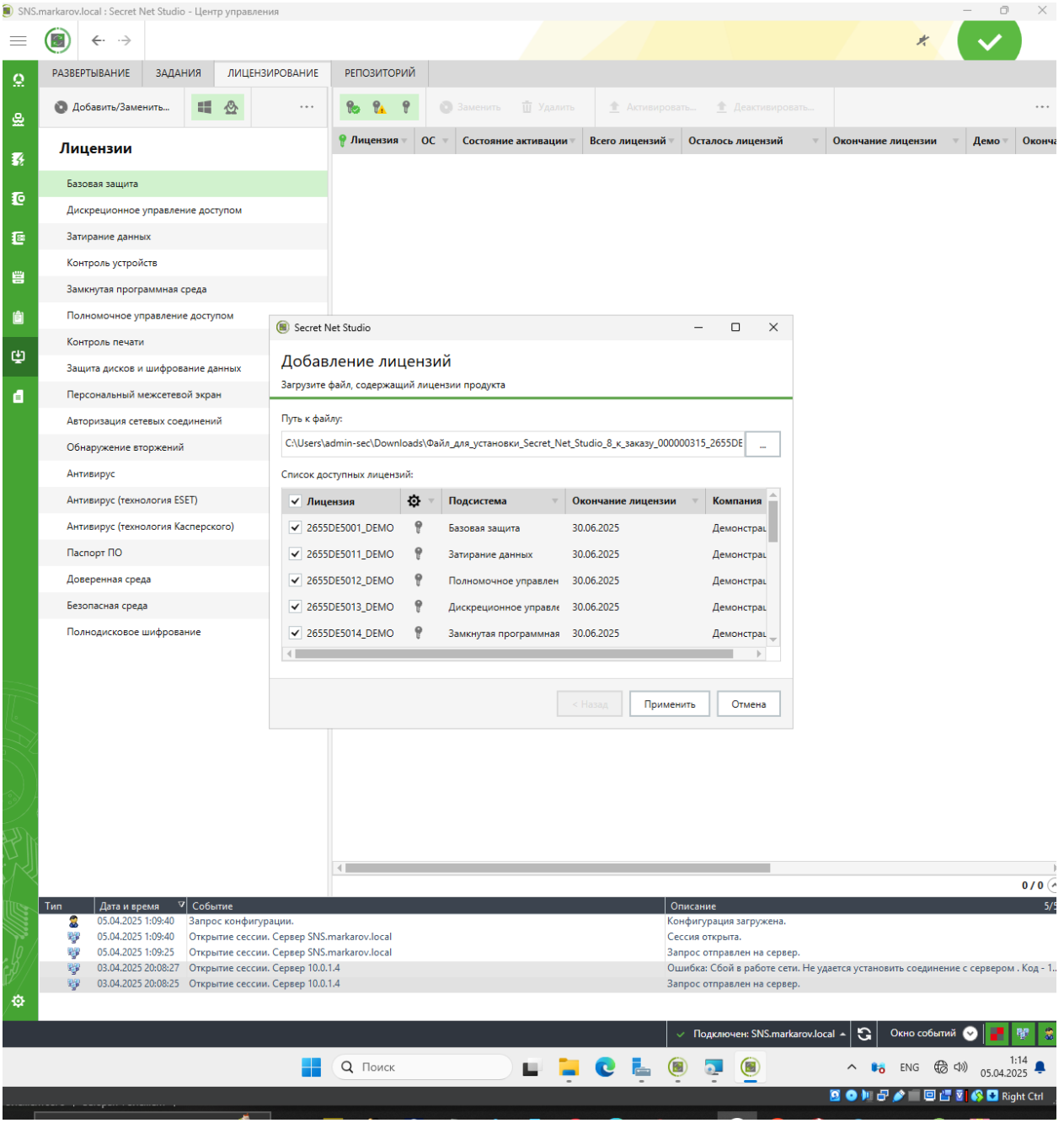

Рис. 17 добавление папки дистрибутивов 8_****

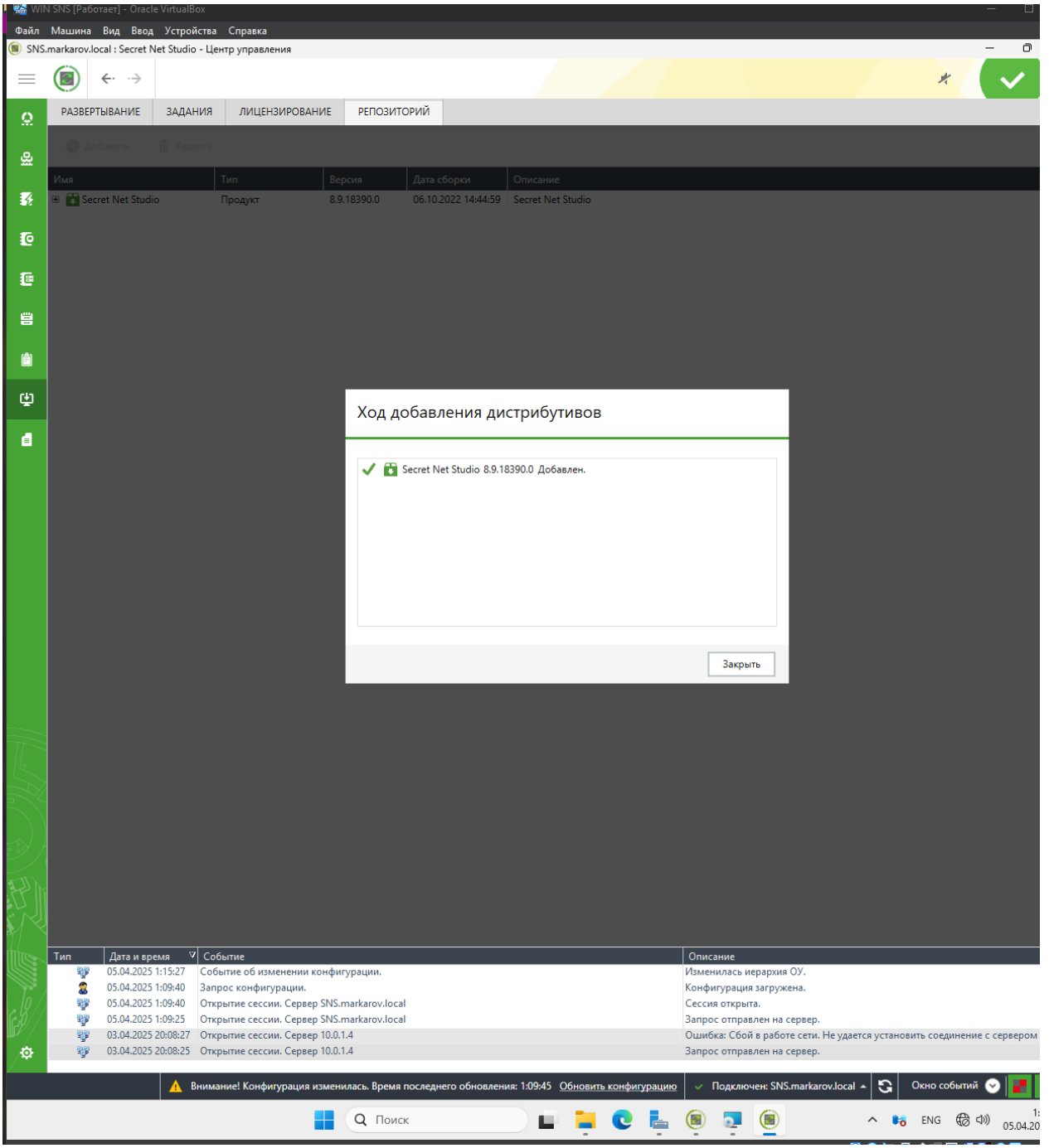

Рис. 18 результат установки

Задание 13.

Для дальнейшей работы у нас высветиться 4 компьютера выбераем компьютер на котором стоит Windows 10 что показанно на рис. 19.

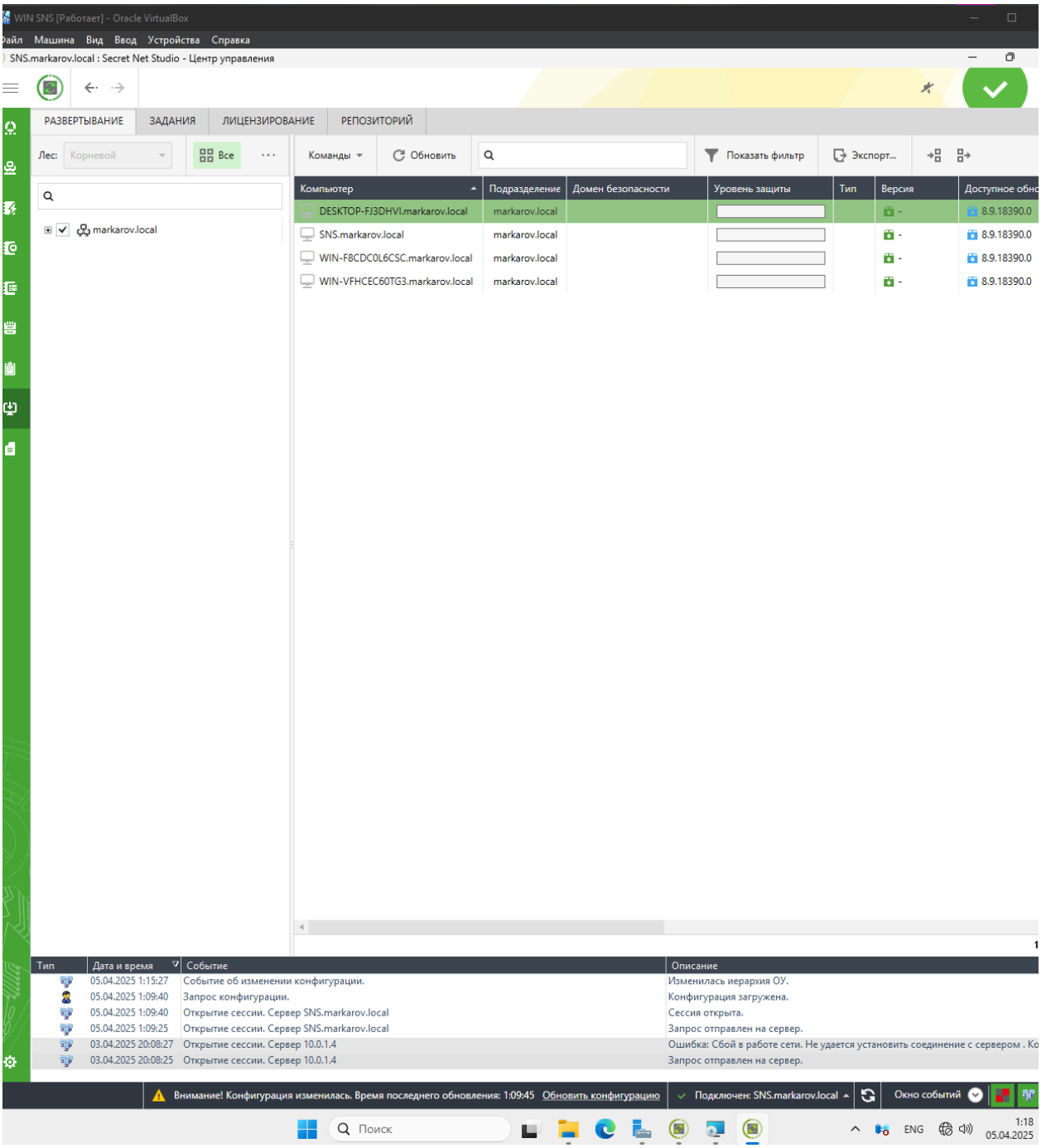

Рис. 19 результат в разделе развёртывание

Дальше устанавливаем на компьютер где Windows 10 пакет secret net studio как показанно на рис. 20

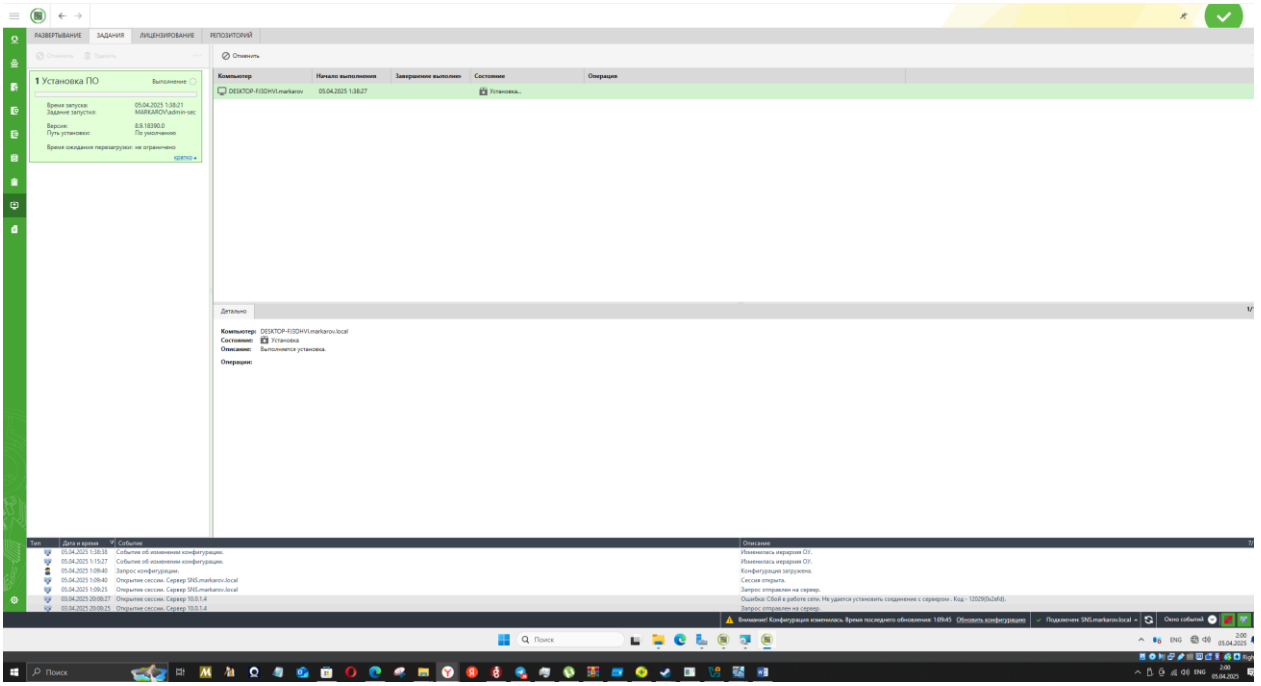

Рис. 20 процесс установки на windows 10 компонент.

Задание 14.

Через центр управления выполнить базовую настройку Secret Net Studio для ПК User. Во вкладке «Контроль устройств» запретить использование USB-носителей как показанно на рис. 21.

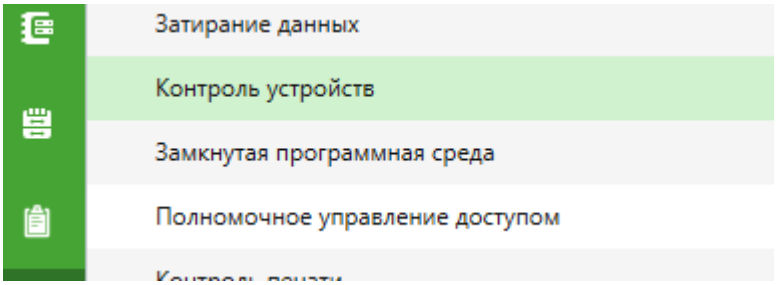

Рисунок 21 Запрещаем устройства

Теоретические вопросы

1. Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации

Техническое обслуживание (ТО) вычислительной техники и других технических средств информатизации включает в себя ряд методов и принципов, которые обеспечивают надежную работу систем. Основные принципы ТО включают:

Плановость и регулярность: ТО должно проводиться согласно заранее установленному графику, что позволяет избежать неожиданных сбоев и продлить срок службы оборудования.

Комплексность: Обслуживание должно охватывать все компоненты системы, включая аппаратное обеспечение, программное обеспечение и сети. Это позволяет выявить и устранить потенциальные проблемы на ранних стадиях.

Прогнозирование и диагностика: Использование методов диагностики для выявления потенциальных неисправностей до их проявления. Это может включать мониторинг состояния оборудования и анализ данных.

Квалификация персонала: Проведение ТО должно осуществляться квалифицированными специалистами, которые обладают необходимыми знаниями и навыками для работы с конкретными системами.

Документирование: Ведение учета всех проведенных работ по техническому обслуживанию, что позволяет отслеживать историю обслуживания и принимать обоснованные решения для будущих действий.

2. Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении

Диагностика систем защиты информации включает в себя:

Анализ угроз и уязвимостей: Регулярное проведение анализа для выявления потенциальных угроз и уязвимостей в системе.

Тестирование и мониторинг: Использование инструментов для тестирования системы на наличие уязвимостей и мониторинга ее состояния в реальном времени.

Устранение отказов: В случае выявления отказов необходимо провести анализ причин, устранить неисправности и выполнить восстановление системы. Это может включать замену компонентов, обновление программного обеспечения или изменение конфигурации.

Восстановление работоспособности: После устранения отказов необходимо провести тестирование системы для подтверждения ее работоспособности и соответствия требованиям безопасности.

3. Настройка и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам

Настройка и устранение неисправностей средств защиты информации в компьютерных сетях включает следующие этапы:

Настройка параметров безопасности: Определение и настройка правил доступа, шифрования данных и других параметров, обеспечивающих защиту информации в сети.

Мониторинг и анализ: Постоянный мониторинг сети на предмет несанкционированного доступа и анализ журналов событий для выявления аномалий.

Устранение неисправностей: В случае возникновения проблем необходимо провести диагностику, выявить источник неисправности и выполнить необходимые действия для ее устранения. Это может включать перезагрузку оборудования, обновление программного обеспечения или изменение конфигурации.

Документирование изменений: Ведение записей о всех произведенных изменениях и настройках для обеспечения возможности последующего анализа и восстановления.

Вывод:

Организация и проведение технического обслуживания, диагностика и устранение неисправностей в системах защиты информации являются ключевыми аспектами обеспечения надежной и безопасной работы автоматизированных систем. Применение системного подхода, регулярное обновление знаний и квалификация персонала позволяют минимизировать риски и повысить эффективность работы оборудования и программного обеспечения.