МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА –Российский технологический университет»
РТУ МИРЭА

Институт кибербезопасности и цифровых технологий

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

Дисциплина «Технологии обеспечения информационной безопасности»

Отчет
о проделанной практической работе №3

Выполнил студент 1 курса
Группы: ББМО-02-24
Худяков Д.А.
Проверил
Петров К. Е.

Москва
2024

Вариант 8

1. Устанавливаем **Security Policy Tool** на компьютер с сайта.

2. **Изучаем встроенные примеры политики доступа (ПД) в приложении, которое мы установили «Security Policy Tool». Например,** меди-цинский центр, университет и т.д.

3. **Определение своего варианта для выполнения задания:**
N = n mod m + 1 = 7 mod 10 + 1 = 7 + 1 = 8 (8 вариант)

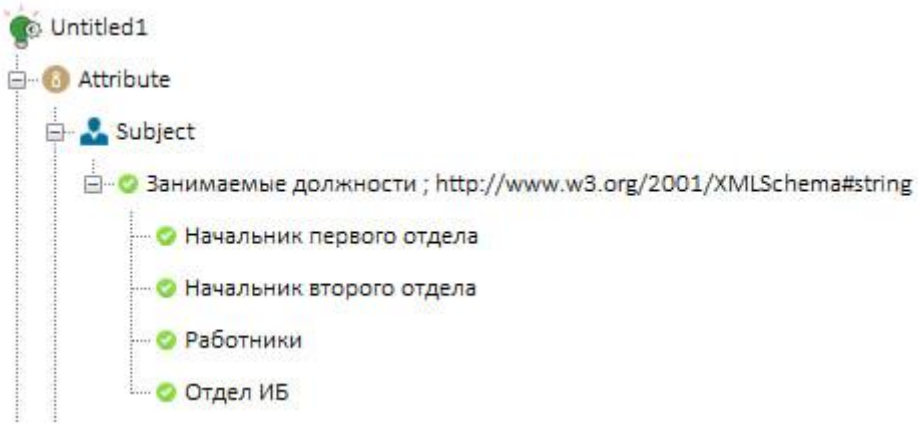
4. **Разработка и верификация ПБ по Заданию №8 из Приложения 1.**

Задание 8

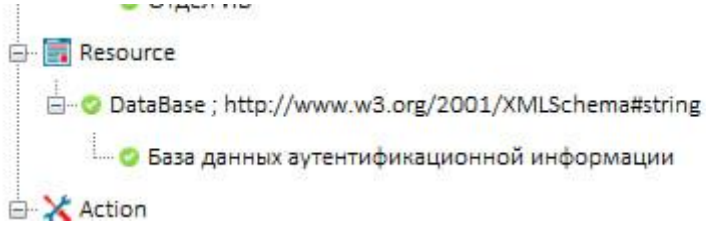
Дано:
Система учета аутентифицирующей информации к автоматизированным рабочим местам.
Субъекты: сотрудник отдела ИБ, начальник отдела (2 субъекта), работники (4 субъекта).
Объект: база данных аутентифицирующей информации.
Задание: Сформировать политику доступа субъектов к базе данных аутентифицирующей информации.
Вопрос: Используя специализированное ПО Security Policy Tool, выяс-ните имеет ли начальник одного отдела иметь доступ и корректировать аутентифицирующею информацию сотрудников другого отдела?

Ход работы:

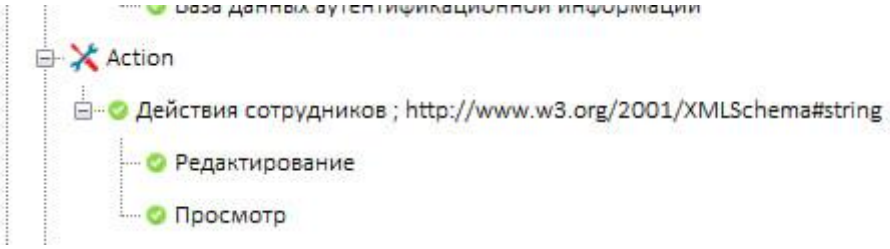
1. Для начала создаем в разделе «Subject» занимаемые должности сотрудников:



2. Далее в раздел «Resource» добавляем базу данных:

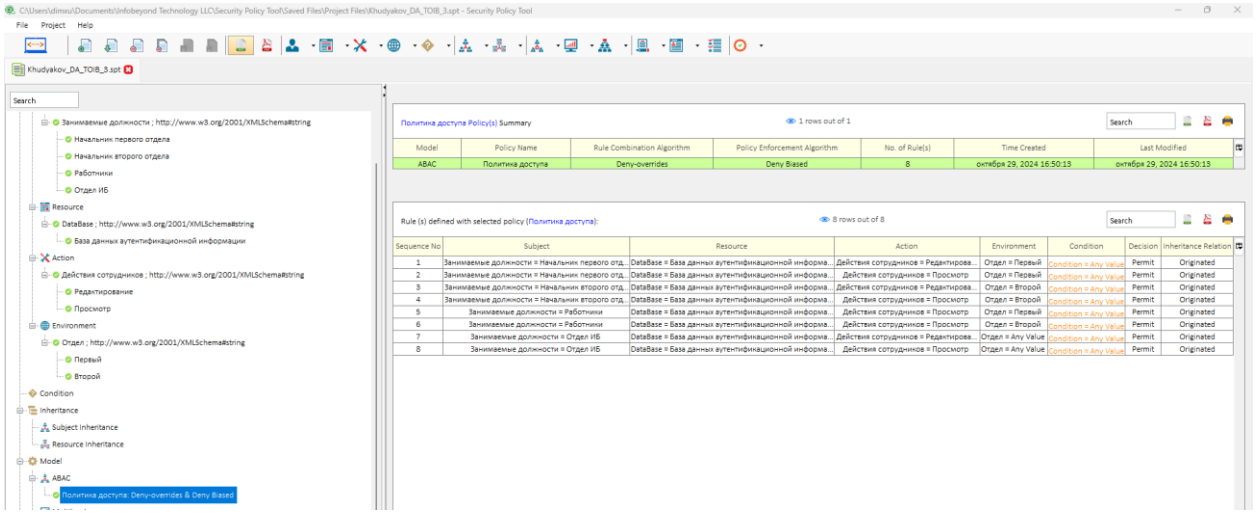


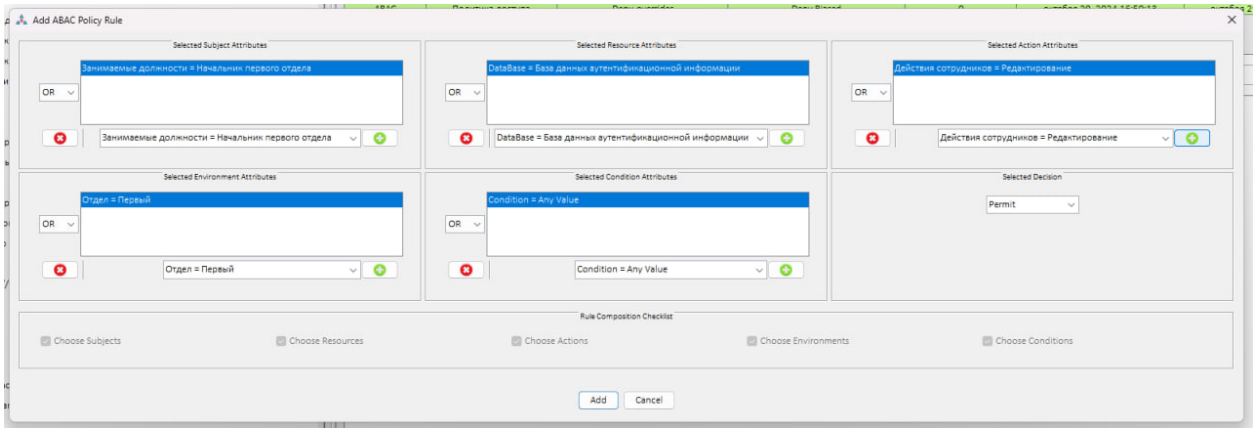
3. В раздел «Action» добавляем возможные действия сотрудников с базой данных аутентифицирующей информации:



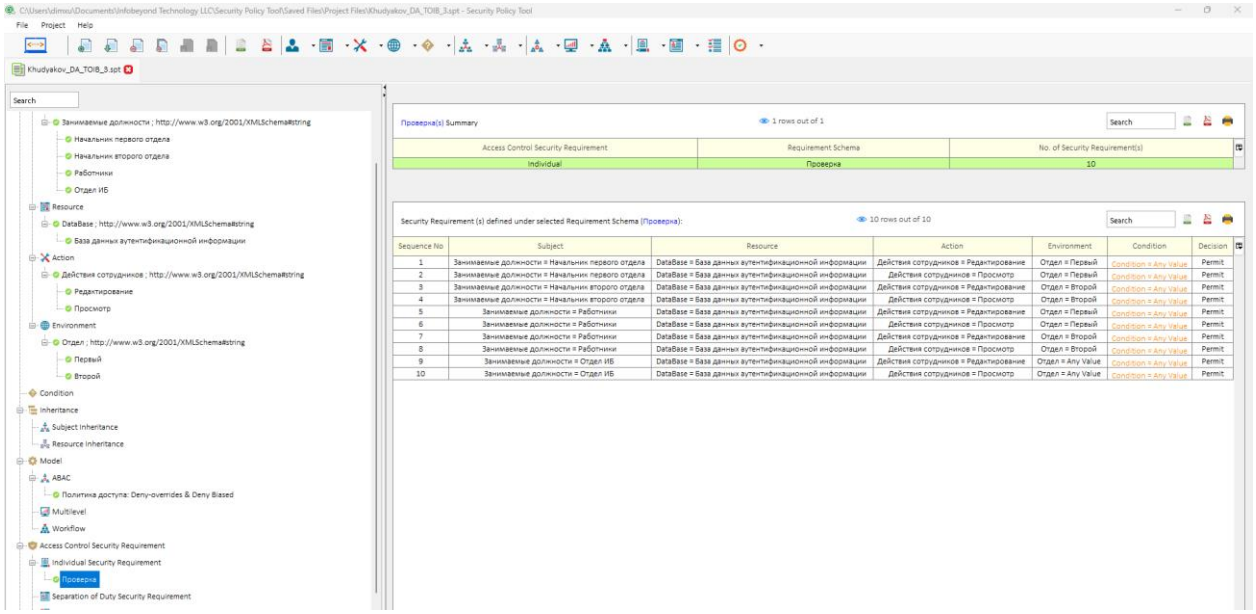
4. В раздел «Environment» добавляем среду их работы (Кто-то в первом отделе работает, а кто-то во втором):

5. Далее в разделе «ABAC» добавляем политику доступа:

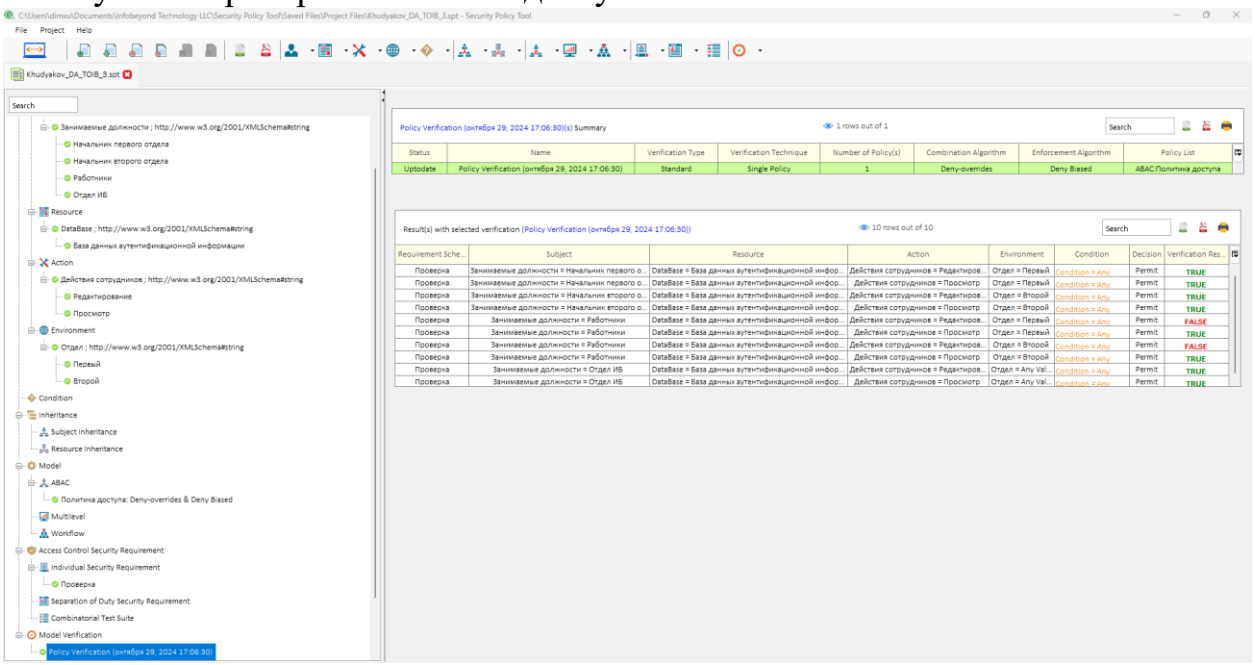




6. В разделе «Individual Security Requirement» производим тестирование всех возможных ситуаций:



7. Результат проверки политики доступа:



Вывод:
1) Начальник первого отдела может просматривать и редактировать аутентифицирующую информацию только первого отдела (Можно увидеть, что после результата проверки у начальника первого отдела нет доступа к аутентифицирующей информации второго отдела)
2) Начальник второго отдела может редактировать и просматривать аутентифицирующую информацию только второго отдела (Можно увидеть, что после результата проверки у начальника второго отдела нет доступа к аутентифицирующей информации первого отдела)
3) А сотрудник отдела ИБ может просматривать и редактировать аутентифицирующую информацию всех отделов (Первого и Второго отдела)
4) Работники, наоборот, не имеют прав на просмотр и редактирование аутентифицирующей информации всех отделов (Первого и Второго отдела)

Таким образом, можно сделать вывод, что результат проверки оказался положительным и такая политика доступа имеет место быть.

Вопрос: Используя специализированное ПО Security Policy Tool, выяс-ните имеет ли начальник одного отдела иметь доступ и корректировать аутентифицирующею информацию сотрудников другого отдела?

Ответ: (Нет) Начальник одного отдела не может иметь доступ и корректировать аутентифицирующую информацию сотрудников другого отдела.