|  |  |  |
| --- | --- | --- |
|  |  |  |
| 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» | | |

**Отчёт по практической работе № 3**

**по дисциплине ««Технологии обеспечения информационной безопасностью»**

**Тема:** «**Разработка политики доступа**»

Выполнил

Студент 1 курса

Группы ББМО-01-23

Белов Владимир Станиславович

Шифр 23Б1716

Вариант 2

Москва 2023

**Цели работы:**

1. Обобщить, закрепить лекционный и теоретический материал по теме.

**Вопросы для самоконтроля и самостоятельной работы:**

**Задание 2.**

Дано: Информационная система хранения личных дел работников. Субъекты: сотрудник отдела кадров, начальники отделов (2 субъекта), работники (4 субъекта).

Объект: база данных личных дел работников. Задание: сформировать политику доступа субъектов к базе данных личных дел.

Вопрос: Используя специализированное ПО Security Policy Tool, выясните может ли работник просматривать личные дела других работников и корректировать свое?

Отчёт по практической работе

Создадим субъектом предприятия, а именно:

* Сотрудника отдела кадров;
* Начальники отделов (2 субъекта);
* Работники отделов (4 субъекта).

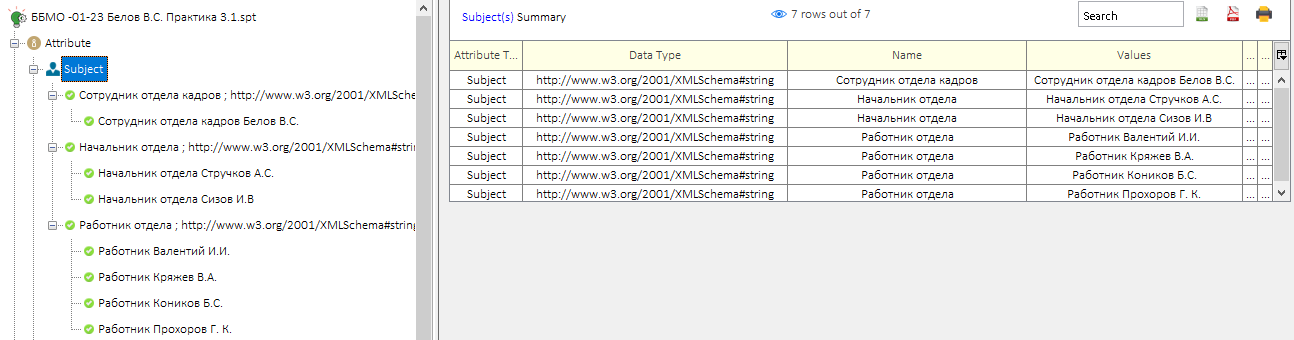


Рисунок 1. – Создание субъектов доступа на предприятии.

Объектом доступа будет являться база данных личных дел работников. Создадим её.

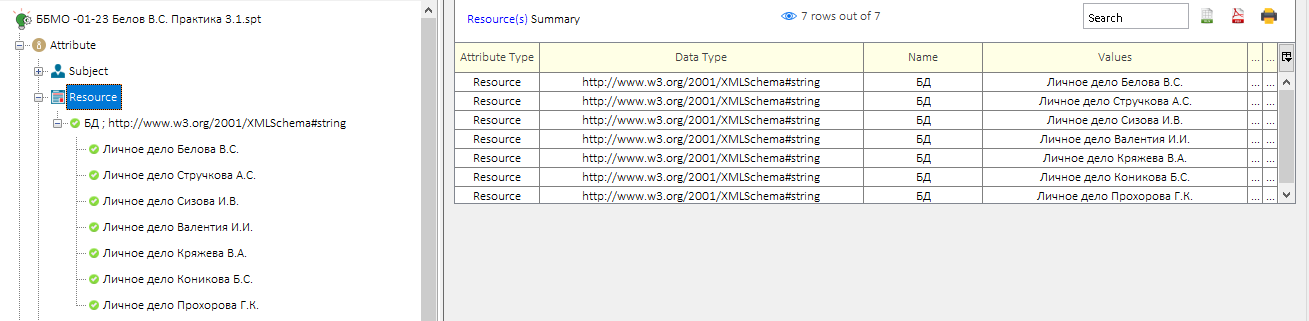


Рисунок 2. - Создание объектов доступа.

Определим действия, которые могут осуществлять субъекты над объектами доступа.

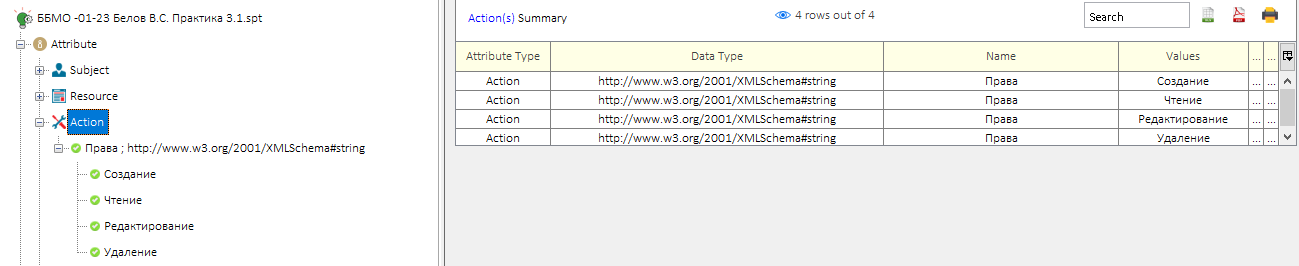


Рисунок 3. - Создание действий над объектами и их аттрибуты.

Далее создадим политику безапостности, учитывая, что за начальником отдела Стручковым А.С. закреплены Валентий И.И. и Кряжев В.А., а за начальником отдела Сизовым И.В: Коников Б.С., Прохоров Г. К. Отметим, что начальники отдела могут просматривать и редактировать дела своих работников, но не сотрудников других отделов. Сотрудник отдела кадров имеет право осуществлять любые действия над работниками предприятия, но может только редактировать и читать собственное дело.

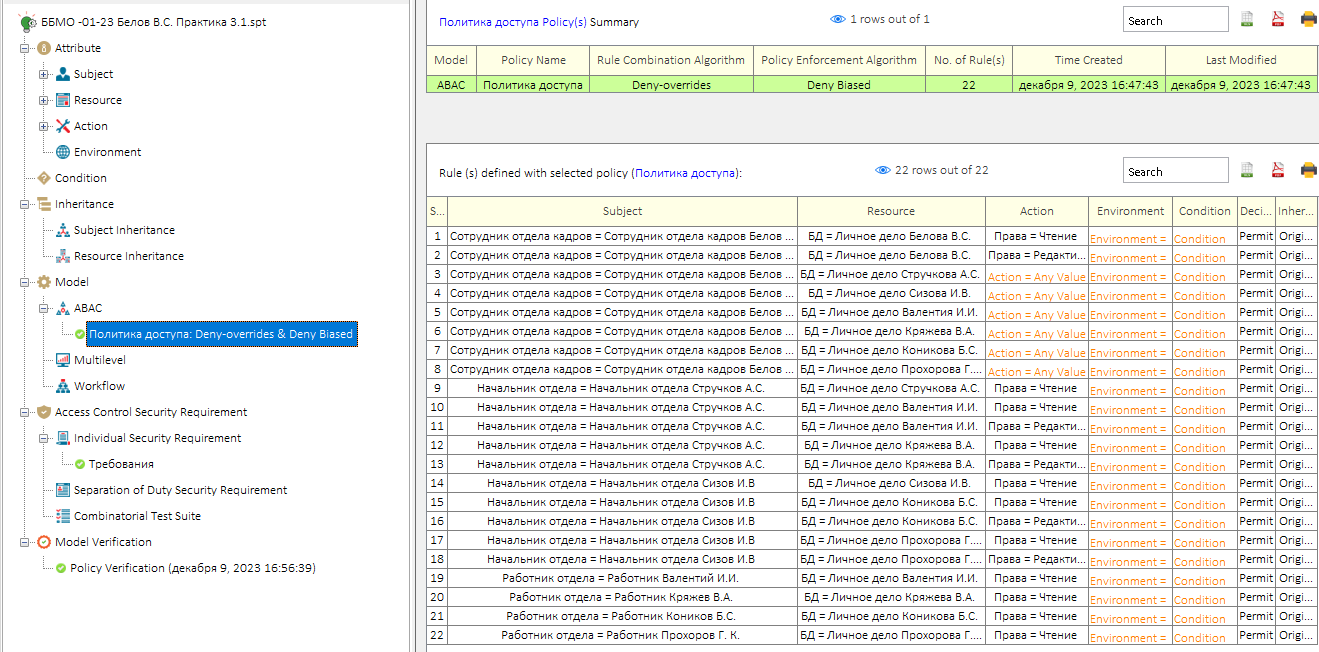


Рисунок 4. - Создание политики безопасности.

Далее создадим требования к безопасности, учитывая что работники не могут взаимодействовать с делами, отличных от своих, начальники отдела могут взаимодействовать с делами своих работников и собственным.

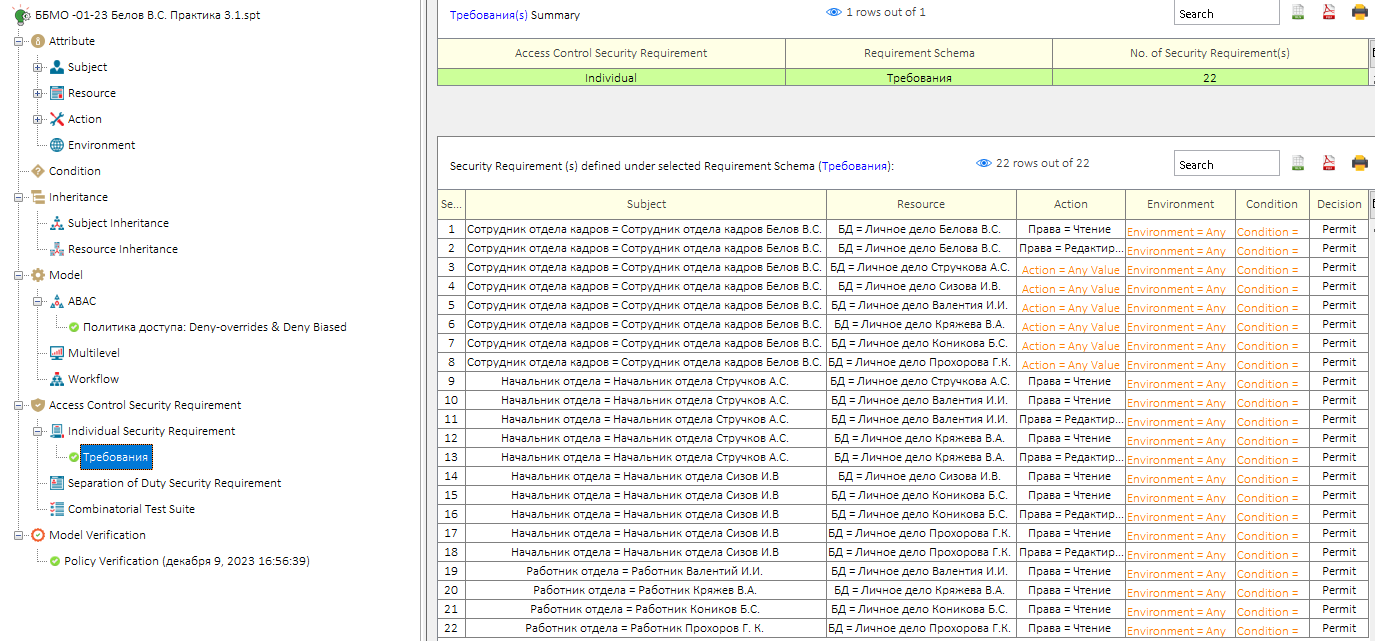


Рисунок 5. - Создание требований безопасности.

Создадим верификацию модели.

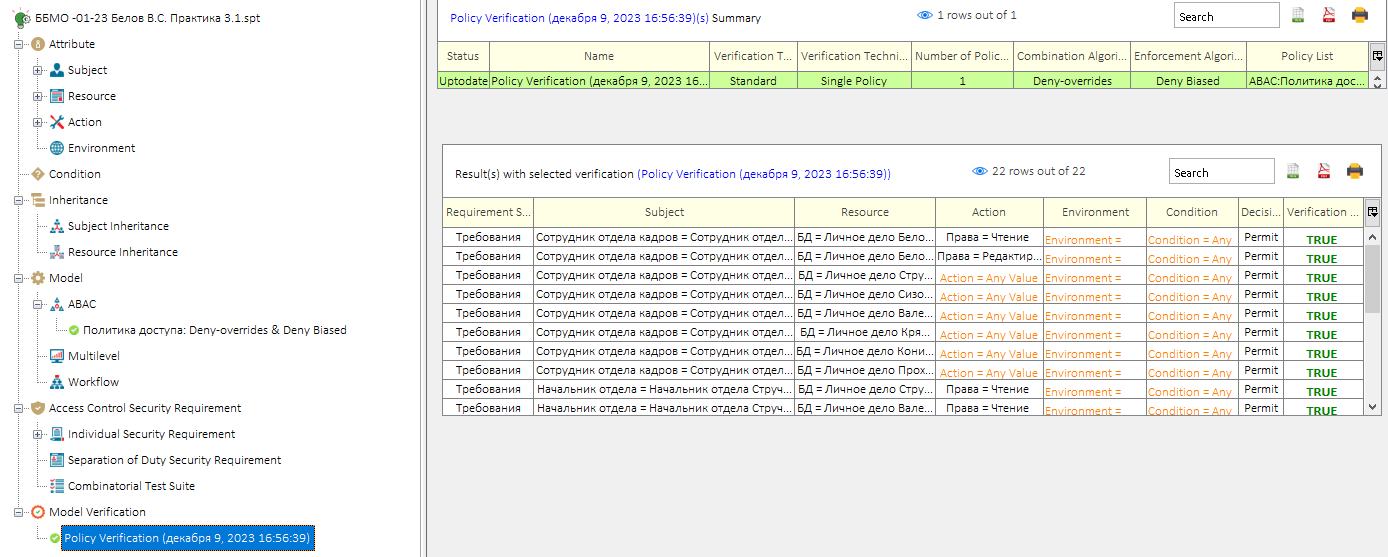


Рисунок 6. - Верификация политики безопасности

Вывод: В результате работы было установлено, что работники не имеют доступа к просмотру чужих личных дел и не могут редактировать своё. Начальники отдела могут редактировать дела своих подчененных и просматривать своё, а сотрудник отдела имеет доступ к любым действиям над сотрдуниками предприятия, за исключением создания и удачелия личных дел.