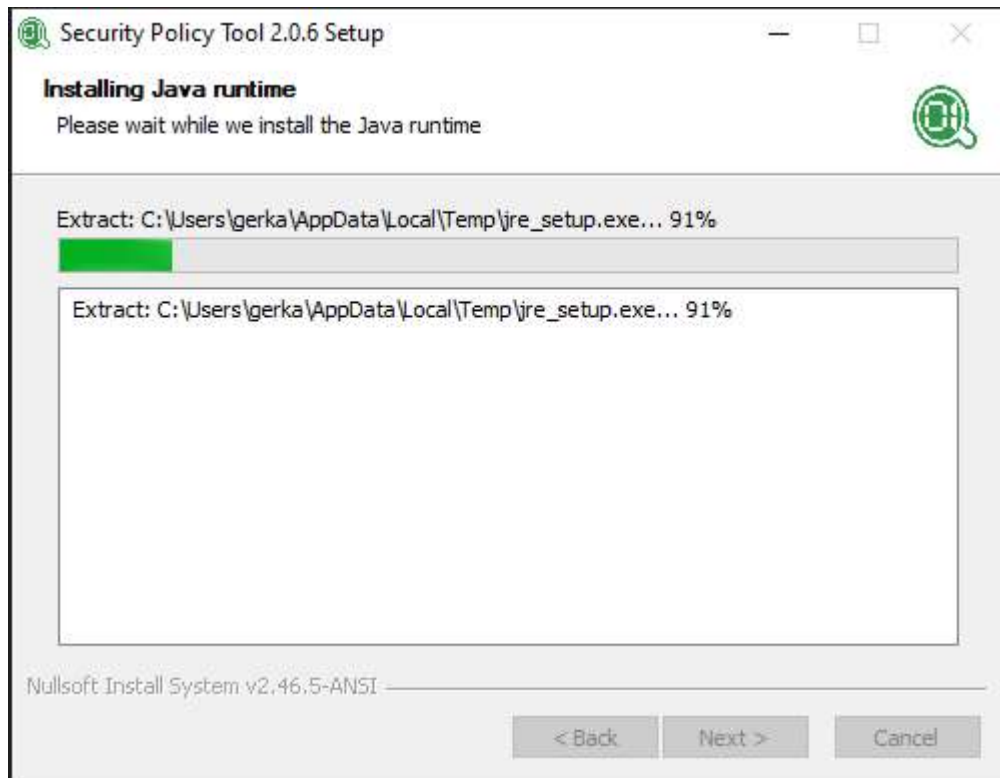


1. Установка Security Policy Tool на компьютер



2. Определение исходных данных

Чурсинов 14ый в списке / $10 + 1 = 5$ вариант

3. Разработка и верификация ПБ

- **Дано:** Система управления доступом к электронному архиву дел
- **Субъекты:** делопроизводитель, работники (4 субъекта), начальники отделов (2 субъекта).
- **Объект:** электронный архив дел.
- **Задание:** сформировать политику доступа субъектов к архиву дел.
- **Вопрос:** Используя специализированное ПО Security Policy Tool, выясните может ли работник просматривать дела другого отдела и удалять дела своего?

3.1. Создание субъектов доступа

Security Policy Tool interface showing a tree view on the left and a table on the right.

Tree View (Left):

- Attribute
 - Subject
 - Деполпроисводитель : http://www.w3.org/2001/XMLSchema#string
 - Деполпроисводитель 1
 - Работник : http://www.w3.org/2001/XMLSchema#string
 - Работник А
 - Работник Б
 - Работник В
 - Работник Г
 - Начальники отделов : http://www.w3.org/2001/XMLSchema#string
 - Начальник Отдела 1
 - Начальник Отдела 2
 - Resource
 - Электронный архив дел : http://www.w3.org/2001/XMLSchema#string
 - Дело 1
 - Дело 2
 - Дело 3
 - Дело 4
 - Дело 5
 - Дело 6
 - Дело 7
 - Action
 - Environment
 - Condition
 - Inheritance
 - Subject Inheritance
 - Resource Inheritance
 - Model
 - ABAC
 - Multilevel
 - Workflow
 - Access Control Security Requirement
 - Individual Security Requirement

Table (Right):

Subjects Summary (7 rows out of 7)

Attribute Type	Data Type	Name	Values	Time Created	Last Updated
Subject	http://www.w3.org/2001/XMLSchema#string	Деполпроисводитель	Деполпроисводитель 1	октябрь 26, 2023 16:59:48	октябрь 26, 2023 17:13:48
Subject	http://www.w3.org/2001/XMLSchema#string	Работник	Работник А	октябрь 26, 2023 16:59:18	октябрь 26, 2023 16:59:18
Subject	http://www.w3.org/2001/XMLSchema#string	Работник	Работник В	октябрь 26, 2023 16:59:33	октябрь 26, 2023 16:59:33
Subject	http://www.w3.org/2001/XMLSchema#string	Работник	Работник В	октябрь 26, 2023 16:59:45	октябрь 26, 2023 16:59:45
Subject	http://www.w3.org/2001/XMLSchema#string	Работник	Работник Г	октябрь 26, 2023 16:59:50	октябрь 26, 2023 16:59:50
Subject	http://www.w3.org/2001/XMLSchema#string	Начальники отделов	Начальник Отдела 1	октябрь 26, 2023 17:00:11	октябрь 26, 2023 17:00:11
Subject	http://www.w3.org/2001/XMLSchema#string	Начальники отделов	Начальник Отдела 2	октябрь 26, 2023 17:00:22	октябрь 26, 2023 17:00:22

3.2. Создание объектов доступа

Security Policy Tool interface showing a tree view on the left and a table on the right.

Tree View (Left):

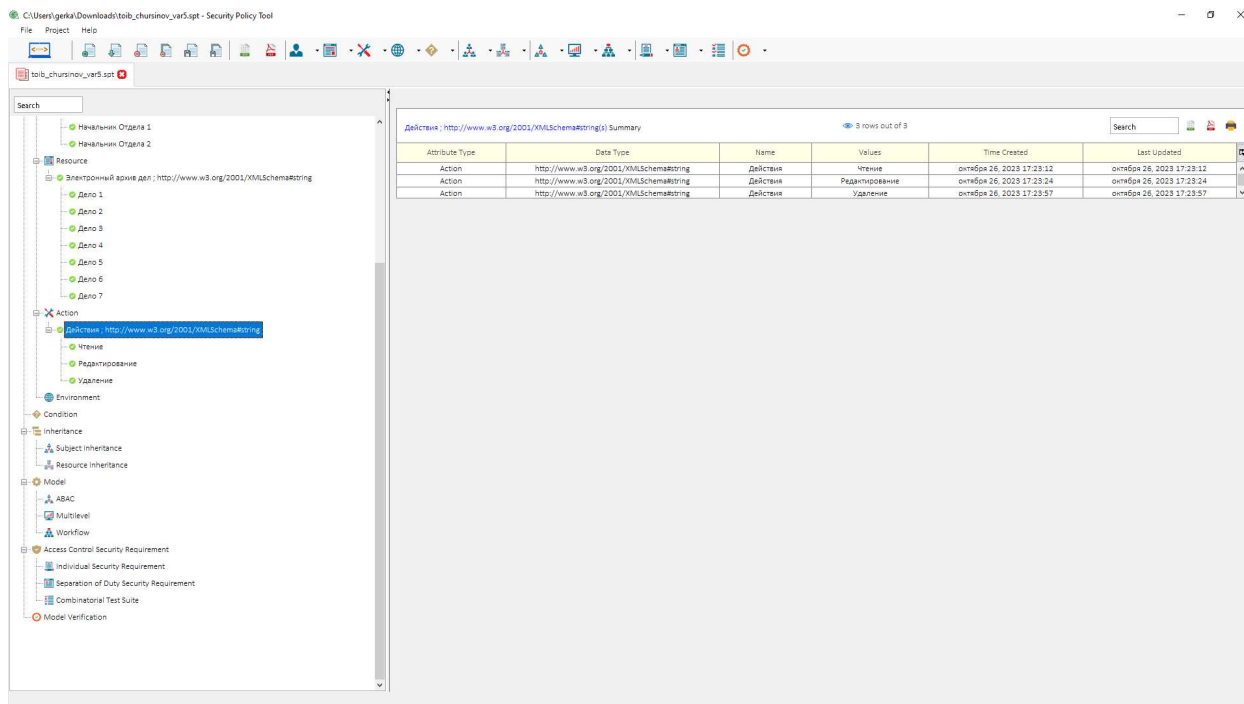
- Attribute
 - Subject
 - Деполпроисводитель : http://www.w3.org/2001/XMLSchema#string
 - Деполпроисводитель 1
 - Работник : http://www.w3.org/2001/XMLSchema#string
 - Работник А
 - Работник Б
 - Работник В
 - Работник Г
 - Начальники отделов : http://www.w3.org/2001/XMLSchema#string
 - Начальник Отдела 1
 - Начальник Отдела 2
 - Resource
 - Электронный архив дел : http://www.w3.org/2001/XMLSchema#string
 - Дело 1
 - Дело 2
 - Дело 3
 - Дело 4
 - Дело 5
 - Дело 6
 - Дело 7
 - Action
 - Environment
 - Condition
 - Inheritance
 - Subject Inheritance
 - Resource Inheritance
 - Model
 - ABAC
 - Multilevel
 - Workflow
 - Access Control Security Requirement
 - Individual Security Requirement

Table (Right):

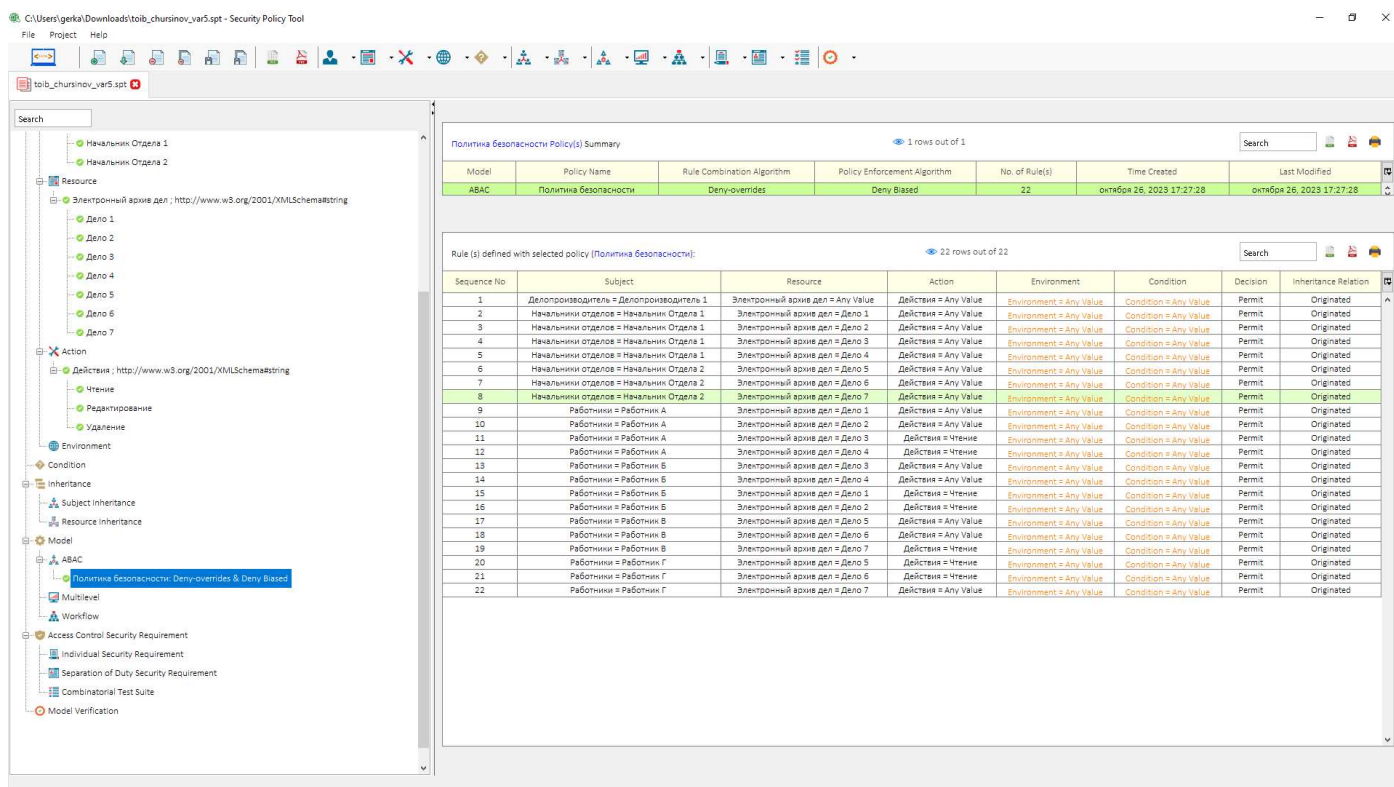
Электронный архив дел : http://www.w3.org/2001/XMLSchema#string Summary (7 rows out of 7)

Attribute Type	Data Type	Name	Values	Time Created	Last Updated
Resource	http://www.w3.org/2001/XMLSchema#string	Электронный архив дел	Дело 1	октябрь 26, 2023 17:15:18	октябрь 26, 2023 17:15:18
Resource	http://www.w3.org/2001/XMLSchema#string	Электронный архив дел	Дело 2	октябрь 26, 2023 17:15:33	октябрь 26, 2023 17:15:33
Resource	http://www.w3.org/2001/XMLSchema#string	Электронный архив дел	Дело 3	октябрь 26, 2023 17:15:39	октябрь 26, 2023 17:15:39
Resource	http://www.w3.org/2001/XMLSchema#string	Электронный архив дел	Дело 4	октябрь 26, 2023 17:15:44	октябрь 26, 2023 17:15:44
Resource	http://www.w3.org/2001/XMLSchema#string	Электронный архив дел	Дело 5	октябрь 26, 2023 17:15:49	октябрь 26, 2023 17:15:49
Resource	http://www.w3.org/2001/XMLSchema#string	Электронный архив дел	Дело 6	октябрь 26, 2023 17:15:56	октябрь 26, 2023 17:15:56
Resource	http://www.w3.org/2001/XMLSchema#string	Электронный архив дел	Дело 7	октябрь 26, 2023 17:16:03	октябрь 26, 2023 17:16:03

3.3. Создание возможных действий



3.4. Создание политики безопасности



Политика безопасности устроена следующим образом:

Делопроизводитель:

- имеет доступ к любому делу любого отдела

Начальник отдела:

- имеет доступ к любому делу только из своего отдела
- не имеет доступ к делу из другого отдела

Работник:

- может читать только дела своего отдела
- может редактировать и удалять только свои дела

3.5. Создание требований безопасности

The screenshot shows the Security Policy Tool interface. The left pane displays a tree structure with the following nodes: Search, Resource (Начальник Отдела 2, Электронный архив дел; http://www.w3.org/2001/XMLSchemaString, Дело 1, Дело 2, Дело 3, Дело 4, Дело 5, Дело 6, Дело 7), Action (Действия; http://www.w3.org/2001/XMLSchemaString, Чтение, Редактирование, Удаление), Environment, Condition, Inheritance (Subject Inheritance, Resource Inheritance), Model (ABAC, Политика безопасности: Deny-overrides & Deny Biased, Multilevel, Workflow), Access Control Security Requirement, Individual Security Requirement (Требования), Separation of Duty Security Requirement, Combinatorial Test Suite, and Model Verification.

The right pane displays the 'Requirements' section. It shows a table with 21 rows of security requirements. The table has the following columns: Sequence No, Subject, Resource, Action, Environment, Condition, and Decision.

Sequence No	Subject	Resource	Action	Environment	Condition	Decision
1	Работники = Работник А	Электронный архив дел = Дело 5	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny
2	Работники = Работник А	Электронный архив дел = Дело 6	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny
3	Работники = Работник А	Электронный архив дел = Дело 7	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny
4	Работники = Работник В	Электронный архив дел = Дело 5	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny
5	Работники = Работник В	Электронный архив дел = Дело 6	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny
6	Работники = Работник В	Электронный архив дел = Дело 7	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny
7	Начальники отделов = Начальник Отдела 1	Электронный архив дел = Дело 5	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny
8	Начальники отделов = Начальник Отдела 1	Электронный архив дел = Дело 6	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny
9	Начальники отделов = Начальник Отдела 1	Электронный архив дел = Дело 7	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny
10	Работники = Работник В	Электронный архив дел = Дело 1	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny
11	Работники = Работник В	Электронный архив дел = Дело 2	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny
12	Работники = Работник В	Электронный архив дел = Дело 3	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny
13	Работники = Работник В	Электронный архив дел = Дело 4	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny
14	Работники = Работник Г	Электронный архив дел = Дело 1	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny
15	Работники = Работник Г	Электронный архив дел = Дело 2	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny
16	Работники = Работник Г	Электронный архив дел = Дело 3	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny
17	Работники = Работник Г	Электронный архив дел = Дело 4	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny
18	Начальники отделов = Начальник Отдела 2	Электронный архив дел = Дело 1	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny
19	Начальники отделов = Начальник Отдела 2	Электронный архив дел = Дело 2	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny
20	Начальники отделов = Начальник Отдела 2	Электронный архив дел = Дело 3	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny
21	Начальники отделов = Начальник Отдела 2	Электронный архив дел = Дело 4	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny

Требования безопасности сформированы следующим образом:

- Сотрудники Отдела 1 (Работник А, Работник Б, Начальник отдела 1) не имеют доступа к делам Отдела 2. (Дело 5, Дело 6, Дело 7)
- Сотрудники Отдела 2 (Работник В, Работник Г, Начальник отдела 2) не имеют доступа к делам Отдела 1. (Дело 1, Дело 2, Дело 3, Дело 4)

3.6. Верификация политики безопасности

The screenshot displays the Security Policy Tool interface. On the left is a tree view of the policy model, including sections for Actions (Чтение, Редактирование, Удаление), Environment, Condition, Inheritance, Model (ABAC, Multilevel, Workflow), Access Control Security Requirement, Individual Security Requirement, Separation of Duty Security Requirement, Combinatorial Test Suite, and Model Verification. The 'Policy Verification' item is selected.

The main area shows the 'Policy Verification (октябрь 26, 2023 17:53:47)' summary. Below this is a table with the following data:

Status	Name	Verification Type	Verification Technique	Number of Policy(s)	Combination Algorithm	Enforcement Algorithm	Policy List
Uptodate	Policy Verification (октябрь 26, 2023 17:53:47)	Standard	Single Policy	1	Deny-overrides	Deny Biased	ABAC:Политика безопасности

Below the summary is a table titled 'Result(s) with selected verification (Policy Verification (октябрь 26, 2023 17:53:47))' showing 21 rows of results:

Requirement Schema	Subject	Resource	Action	Environment	Condition	Decision	Verification Result
Требования	Работники = Работник А	Электронный архив дел = Дело 5	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny	TRUE
Требования	Работники = Работник А	Электронный архив дел = Дело 6	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny	TRUE
Требования	Работники = Работник А	Электронный архив дел = Дело 7	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny	TRUE
Требования	Работники = Работник Б	Электронный архив дел = Дело 5	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny	TRUE
Требования	Работники = Работник Б	Электронный архив дел = Дело 6	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny	TRUE
Требования	Работники = Работник Б	Электронный архив дел = Дело 7	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny	TRUE
Требования	Начальники отделов = Начальник Отдела 1	Электронный архив дел = Дело 5	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny	TRUE
Требования	Начальники отделов = Начальник Отдела 1	Электронный архив дел = Дело 6	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny	TRUE
Требования	Начальники отделов = Начальник Отдела 1	Электронный архив дел = Дело 7	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny	TRUE
Требования	Работники = Работник В	Электронный архив дел = Дело 1	Действия = Any Value	Environment = Any Value	Condition = Any Value	Deny	TRUE

Согласно верификации модели, все требования были выполнены.

4. Ответ на вопрос преподавателя

- Может ли работник просматривать дела другого отдела и удалять дела своего?
- Нет, работник не может просматривать дела другого отдела, а удалять может

только свои дела. Дела своих коллег он может только просматривать.