



**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, медицинский центр, университет и т.д.
3. Определение своего варианта для выполнения задания:  
$$N = n \bmod m + 1 = 7 \bmod 10 + 1 = 7 + 1 = 8 \text{ (8 вариант)}$$
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.

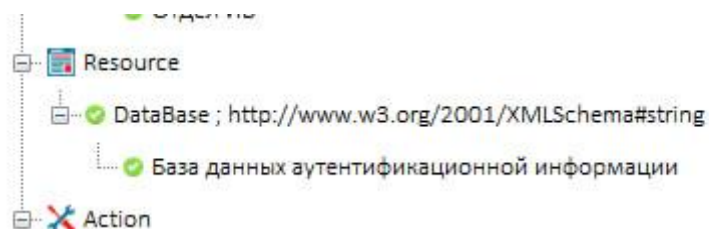
**Вопрос:** Используя специализированное ПО **Security Policy Tool**, выясните имеет ли начальник одного отдела доступ и корректировать аутентифицирующую информацию сотрудников другого отдела?

## Ход работы:

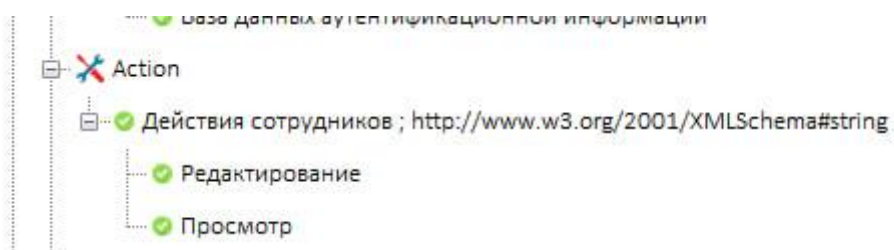
1. Для начала создаем в разделе «Subject» занимаемые должности сотрудников:



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 «АВАС» добавляем политику доступа:

С:\Users\idm\Documents\InfoBeyond Technology LLC\Security Policy Tool\Saved Files\Project Files\Khudyakov\_DA\_TOIB\_3.spt - Security Policy Tool

File Project Help

khudyakov\_DA\_TOIB\_3.spt

Search

- Занимаемые должности; http://www.w3.org/2001/XMLSchema#string
  - Начальник первого отдела
  - Начальник второго отдела
  - Работники
  - Отдел ИБ
- Resource
  - Database; http://www.w3.org/2001/XMLSchema#string
    - База данных аутентификационной информации
- Action
  - Действия сотрудников; http://www.w3.org/2001/XMLSchema#string
    - Редктирование
    - Просмотр
- Environment
  - Отдел; http://www.w3.org/2001/XMLSchema#string
    - Первый
    - Второй
- Condition
- Inheritance
  - Subject Inheritance
  - Resource Inheritance
- Model
  - ABAC
    - Политика доступа: Deny-overrides & Deny Biased

Политика доступа Policy(s) Summary 1 rows out of 1

Model	Policy Name	Rule Combination Algorithm	Policy Enforcement Algorithm	No. of Rule(s)	Time Created	Last Modified
ABAC	Политика доступа	Deny-overrides	Deny Biased	8	октябрь 29, 2024 16:50:13	октябрь 29, 2024 16:50:13

Rule (s) defined with selected policy (Политика доступа): 8 rows out of 8

Sequence No	Subject	Resource	Action	Environment	Condition	Decision	Inheritance Relation
1	Занимаемые должности = Начальник первого отд.	Database = База данных аутентификационной информа.	Действия сотрудников = Редктирование	Отдел = Первый	Condition = Any Value	Permit	Originated
2	Занимаемые должности = Начальник первого отд.	Database = База данных аутентификационной информа.	Действия сотрудников = Просмотр	Отдел = Первый	Condition = Any Value	Permit	Originated
3	Занимаемые должности = Начальник второго отд.	Database = База данных аутентификационной информа.	Действия сотрудников = Редктирование	Отдел = Второй	Condition = Any Value	Permit	Originated
4	Занимаемые должности = Начальник второго отд.	Database = База данных аутентификационной информа.	Действия сотрудников = Просмотр	Отдел = Второй	Condition = Any Value	Permit	Originated
5	Занимаемые должности = Работники	Database = База данных аутентификационной информа.	Действия сотрудников = Просмотр	Отдел = Первый	Condition = Any Value	Permit	Originated
6	Занимаемые должности = Работники	Database = База данных аутентификационной информа.	Действия сотрудников = Просмотр	Отдел = Второй	Condition = Any Value	Permit	Originated
7	Занимаемые должности = Отдел ИБ	Database = База данных аутентификационной информа.	Действия сотрудников = Редктирование	Отдел = Any Value	Condition = Any Value	Permit	Originated
8	Занимаемые должности = Отдел ИБ	Database = База данных аутентификационной информа.	Действия сотрудников = Просмотр	Отдел = Any Value	Condition = Any Value	Permit	Originated

Add ABAC Policy Rule

Selected Subject Attributes

OR

Занимаемые должности = Начальник первого отдела

Selected Resource Attributes

OR

Database = База данных аутентификационной информации

Selected Action Attributes

OR

Действия сотрудников = Редктирование

Selected Environment Attributes

OR

Отдел = Первый

Selected Condition Attributes

OR

Condition = Any Value

Selected Decision

Permit

Rule Composition Checklist

☒ Choose Subjects ☒ Choose Resources ☒ Choose Actions ☒ Choose Environments ☒ Choose Conditions

Add Cancel

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

С:\Users\idm\Documents\InfoBeyond Technology LLC\Security Policy Tool\Saved Files\Project Files\Khudyakov\_DA\_TOIB\_3.spt - Security Policy Tool

File Project Help

khudyakov\_DA\_TOIB\_3.spt

Search

- Занимаемые должности; http://www.w3.org/2001/XMLSchema#string
  - Начальник первого отдела
  - Начальник второго отдела
  - Работники
  - Отдел ИБ
- Resource
  - Database; http://www.w3.org/2001/XMLSchema#string
    - База данных аутентификационной информации
- Action
  - Действия сотрудников; http://www.w3.org/2001/XMLSchema#string
    - Редктирование
    - Просмотр
- Environment
  - Отдел; http://www.w3.org/2001/XMLSchema#string
    - Первый
    - Второй
- Condition
- Inheritance
  - Subject Inheritance
  - Resource Inheritance
- Model
  - ABAC
    - Политика доступа: Deny-overrides & Deny Biased
  - Workflow
  - Access Control Security Requirement
    - Individual Security Requirement
      - Проверка
    - Separation of Duty Security Requirement

Проверка(s) Summary 1 rows out of 1

Access Control Requirement	Requirement Schema	No. of Security Requirement(s)
Individual	Проверка	10

Security Requirement (s) defined under selected Requirement Schema (Проверка): 10 rows out of 10

Sequence No	Subject	Resource	Action	Environment	Condition	Decision
1	Занимаемые должности = Начальник первого отдела	Database = База данных аутентификационной информации	Действия сотрудников = Редктирование	Отдел = Первый	Condition = Any Value	Permit
2	Занимаемые должности = Начальник первого отдела	Database = База данных аутентификационной информации	Действия сотрудников = Просмотр	Отдел = Первый	Condition = Any Value	Permit
3	Занимаемые должности = Начальник второго отдела	Database = База данных аутентификационной информации	Действия сотрудников = Редктирование	Отдел = Второй	Condition = Any Value	Permit
4	Занимаемые должности = Начальник второго отдела	Database = База данных аутентификационной информации	Действия сотрудников = Просмотр	Отдел = Второй	Condition = Any Value	Permit
5	Занимаемые должности = Работники	Database = База данных аутентификационной информации	Действия сотрудников = Редктирование	Отдел = Первый	Condition = Any Value	Permit
6	Занимаемые должности = Работники	Database = База данных аутентификационной информации	Действия сотрудников = Просмотр	Отдел = Первый	Condition = Any Value	Permit
7	Занимаемые должности = Работники	Database = База данных аутентификационной информации	Действия сотрудников = Редктирование	Отдел = Второй	Condition = Any Value	Permit
8	Занимаемые должности = Работники	Database = База данных аутентификационной информации	Действия сотрудников = Просмотр	Отдел = Второй	Condition = Any Value	Permit
9	Занимаемые должности = Отдел ИБ	Database = База данных аутентификационной информации	Действия сотрудников = Редктирование	Отдел = Any Value	Condition = Any Value	Permit
10	Занимаемые должности = Отдел ИБ	Database = База данных аутентификационной информации	Действия сотрудников = Просмотр	Отдел = Any Value	Condition = Any Value	Permit

7. Результат проверки политики доступа:

Search

Занимаемые должности ; http://www.w3.org/2001/XMLSchema#string

Начальник первого отдела

Начальник второго отдела

Работники

Отдел ИБ

Resource

DataBase ; http://www.w3.org/2001/XMLSchema#string

База данных аутентификационной информации

Action

Действия сотрудников ; http://www.w3.org/2001/XMLSchema#string

Редактирование

Просмотр

Environment

Отдел ; http://www.w3.org/2001/XMLSchema#string

Первый

Второй

Condition

Inheritance

Subject Inheritance

Resource Inheritance

Model

ABAC

Политика доступа: Deny-overrides & Deny Biased

Multilevel

Workflow

Access Control Security Requirement

Individual Security Requirement

Проверка

Separation of Duty Security Requirement

Combinatorial Test Suite

Model Verification

Policy verification (oct6Box 29, 2024 17:06:30)

Policy Verification (oct6Box 29, 2024 17:06:30)(s) Summary

1 rows out of 1

Search

Status	Name	Verification Type	Verification Technique	Number of Policy(s)	Combination Algorithm	Enforcement Algorithm	Policy List
Update	Policy Verification (oct6Box 29, 2024 17:06:30)	Standard	Single Policy	1	Deny-overrides	Deny Biased	ABAC/Политика доступа

Result(s) with selected verification (Policy Verification (oct6Box 29, 2024 17:06:30))

10 rows out of 10

Search

Requirement Schem	Subject	Resource	Action	Environment	Condition	Decision	Verification Res.
Проверка	Занимаемые должности » Начальник первого о.	DataBase » База данных аутентификационной инфор.	Действия сотрудников » Редактиров.	Отдел » Первый	Condition » Any	Permit	TRUE
Проверка	Занимаемые должности » Начальник первого о.	DataBase » База данных аутентификационной инфор.	Действия сотрудников » Просмотр	Отдел » Первый	Condition » Any	Permit	TRUE
Проверка	Занимаемые должности » Начальник второго о.	DataBase » База данных аутентификационной инфор.	Действия сотрудников » Редактиров.	Отдел » Второй	Condition » Any	Permit	TRUE
Проверка	Занимаемые должности » Начальник второго о.	DataBase » База данных аутентификационной инфор.	Действия сотрудников » Просмотр	Отдел » Второй	Condition » Any	Permit	TRUE
Проверка	Занимаемые должности » Работники	DataBase » База данных аутентификационной инфор.	Действия сотрудников » Редактиров.	Отдел » Первый	Condition » Any	Permit	FALSE
Проверка	Занимаемые должности » Работники	DataBase » База данных аутентификационной инфор.	Действия сотрудников » Просмотр	Отдел » Первый	Condition » Any	Permit	TRUE
Проверка	Занимаемые должности » Работники	DataBase » База данных аутентификационной инфор.	Действия сотрудников » Редактиров.	Отдел » Второй	Condition » Any	Permit	FALSE
Проверка	Занимаемые должности » Работники	DataBase » База данных аутентификационной инфор.	Действия сотрудников » Просмотр	Отдел » Второй	Condition » Any	Permit	TRUE
Проверка	Занимаемые должности » Отдел ИБ	DataBase » База данных аутентификационной инфор.	Действия сотрудников » Редактиров.	Отдел » Any Val.	Condition » Any	Permit	TRUE
Проверка	Занимаемые должности » Отдел ИБ	DataBase » База данных аутентификационной инфор.	Действия сотрудников » Просмотр	Отдел » Any Val.	Condition » Any	Permit	TRUE

**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, выясните имеет ли начальник одного отдела доступ и корректировать аутентифицирующую информацию сотрудников другого отдела?

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