

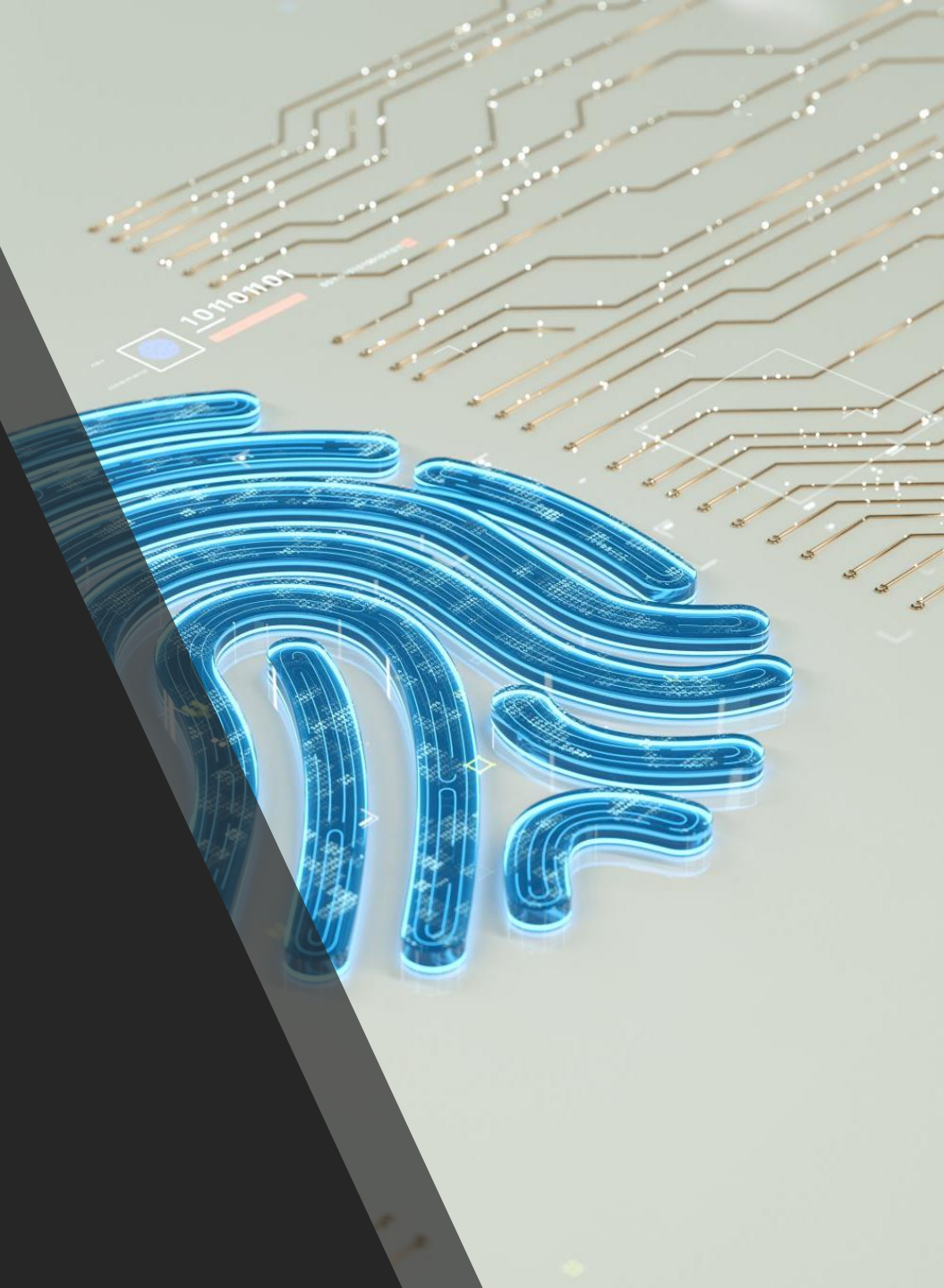
Идентификация и аутентификация. Управление доступом.

ВЫПОЛНИЛА:

ПОНОМАРЕВА ЛИЛИЯ МИХАЙЛОВНА

1032192953

НПИБД-02-19



Содержание

- Идентификация и аутентификация
- Методы аутентификации
- Модели управления доступом
- Заключение

Идентификация и аутентификация

- **Идентификация** – процедура опознавания пользователя по предъявленному *идентификатору* (некое уникальное количество информации, позволяющее различать субъекты и объекты доступа).
- **Аутентификация** – установление подлинности идентифицированного пользователя.

Подтверждение подлинности

Для аутентификации используются:

- парольная информация;
- физический носитель;
- биометрическая характеристика пользователя.

Парольная аутентификация

Достоинство – простота и привычность.

Недостаток – низкий уровень безопасности.

Способы повышения надежности парольной защиты:

- технические ограничения;
- установленный срок действия паролей;
- ограниченное число неудачных попыток входа в систему;
- использование программных генераторов паролей.

Аппаратные средства аутентификации

- Это небольшие по размеру устройства, которые позволяют пользователю получать доступ к информационным системам с локального рабочего места или удаленно с использованием подключения к сети интернет.
- Такие устройства принято называть *токенами*.

Биометрия

- Биометрия представляет собой совокупность автоматизированных методов аутентификации людей на основе их физиологических и поведенческих характеристик.

Управление доступом

Средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты могут выполнять над объектами.

- Физическое управление доступом
- Логическое управление доступом

Управление доступом

- **Цель** управления доступом – это ограничение операций которые может проводить легитимный пользователь.
- Управление доступом указывает что конкретно пользователь имеет право делать в системе, а также какие операции разрешены для выполнения приложениями, выступающими от имени пользователя.

Модели управления доступом

- Дискреционное управление доступом
- Мандатное управление доступом
- Ролевое управление доступом

Дискреционное управление доступом

- Дискреционное (избирательное) управление доступом (англ. discretionary access control, DAC) – управление доступом субъектов к объектам на основе списков управления доступом или матрицы доступа.

Матрица доступа (access control matrix)

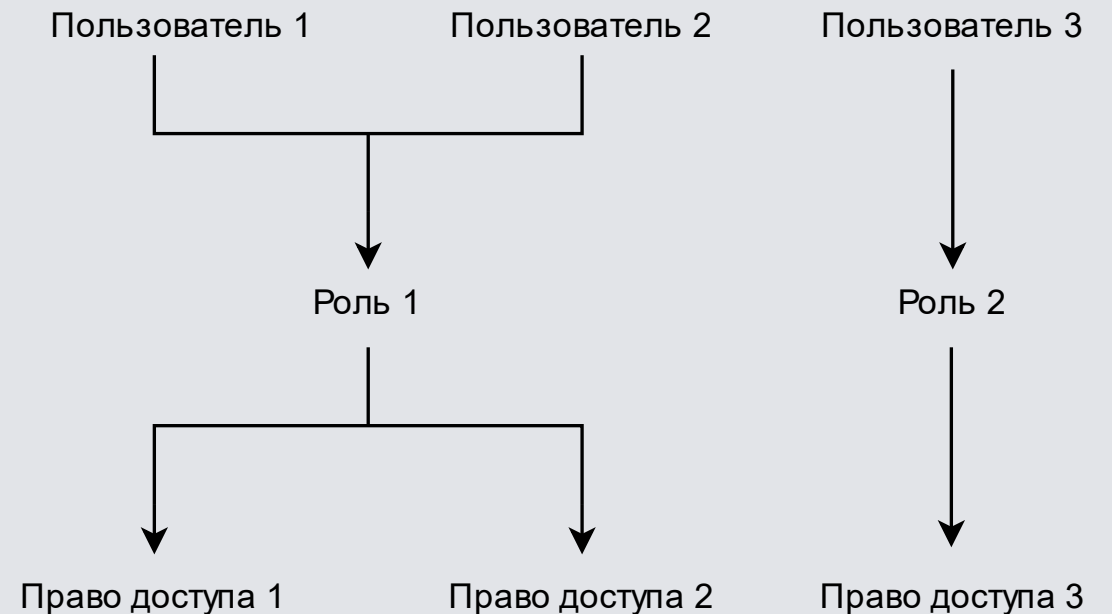
	OS	Accounting Program	Accounting Data	Insurance Data	Payroll Data
Alice	rx	rx	r	-	-
Bob	rx	rx	r	rw	rw
Sam	rwX	rwX	rw	rw	rw

Мандатное управление доступом

- Мандатное (полномочное) управление доступом (англ. Mandatory access control, MAC) – разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений субъектам на обращение к информации такого уровня конфиденциальности.

Ролевое управление доступом

- Управление доступом на основе ролей (англ. Role Based Access Control, RBAC) – развитие политики избирательного управления доступом, в котором права доступа субъектов системы на объекты группируются с учётом специфики их применения, образуя роли.



Заключение

- Основные средства аутентификации: парольная информация, физический носитель, биометрическая характеристика пользователя.
- Модели управления доступом: избирательное управление доступом, полномочное управление доступом, ролевое управление доступом.

Список литературы

- Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — URL: <https://profspo.ru/books/97562> (дата обращения: 16.10.2022).
- Щеглов А.Ю. Модели, методы и средства контроля доступа к ресурсам вычислительных систем : учебное пособие / Щеглов А.Ю.. — Санкт-Петербург : Университет ИТМО, 2014.