Идентификация и аутентификация. Управление доступом.

Доклад по предмету ‘Информационная безопсносность’

Парфенова Елизавета Евгеньевна

Содержание

Список иллюстраций

Список таблиц

1 Введение

В современном мире, где данные становятся важнейшим ресурсом, проблема их защиты выходит на первый план. Быстрая цифровизация бизнес-процессов и повсеместное распространение удаленной работы усиливают требования к защите информации. Компании, работающие с конфиденциальными данными, должны обеспечивать высокие стандарты безопасности для предотвращения несанкционированного доступа. В таких условиях идентификация и аутентификация, а также управление доступом становятся важными инструментами в обеспечении целостности и безопасности данных, что делает изучение и внедрение данных технологий крайне актуальными в современных условиях.

2 Цель работы

Целью данного доклада является ознакомление с понятиями идентификации и аутентификации, их классификацией, типовой схемой этих процессов, а также краткое описание наиболее популярных методов. Кроме того, будет рассмотрено управление доступом, включая его основные задачи, распространенные модели и технологии.

3 Задачи

- Познакомиться с понятиями идентификации и аутентификации, рассмотреть их классификацию
- Рассмотреть типовую схему этих процессов
- Кратко описать два популярных метода аутентификации
- Изучить задачи управления доступом
- Обозначить распространенные модели и технологии управления доступом

4 Идентификация и аутентификация

Идентификация и аутентификация являются ключевыми компонентами систем безопасности, обеспечивая защиту информации и контроль доступа к ресурсам. Эти процессы формируют первую линию обороны в информационном пространстве организаций.

Идентификация - это процесс присвоения уникального идентификатора субъектам и объектам доступа, который затем сравнивается с заданным перечнем. Основные функции идентификации включают:

- установление подлинности и определение полномочий субъекта при его допуске в систему,
- контролирование установленных полномочий в процессе сеанса работы;
- регистрация действий пользователя

Аутентификация (установление подлинности) - проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает. [1]

Один из вариантов процедуры идентификации и аутентификации пользователя представлена на следующем рисунке (рис. 4.1)

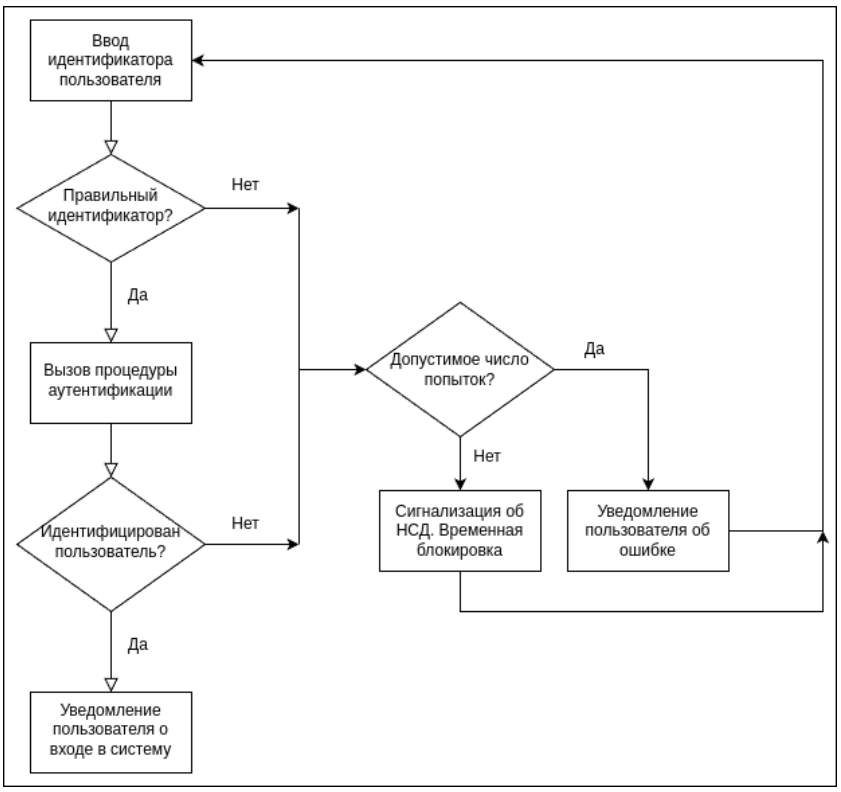

Рис. 4.1: Классическая процедура аутентификации-идентификации

Существует несколько способов подтверждения подлинности субъектом:

- Знание — информация, которую знает субъект. Например пароль, ПИН-код, код, контрольное слово и так далее;
- Владение — вещь, которой обладает субъект. Например электронная или магнитная карта, токен, флеш-память;
- Часть субъекта (биометрия)- свойство, которым обладает субъект: голос, отпечатки пальцев, радужная оболочка глаза, уникальные отличия; [2]

Более подробно способы идентификации и аутентификации представлена на следующем рисунке (рис. 4.2):

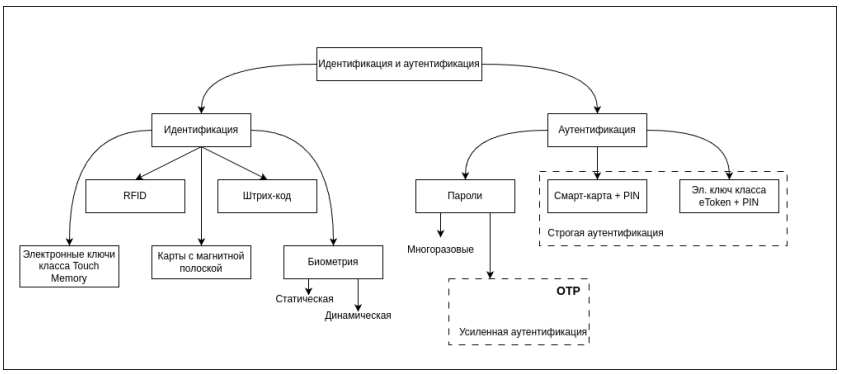

Рис. 4.2: Способы идентификации-аутентификации

Аутентификацию можно классифицировать по нескольким признакам:

1. Односторонняя и двусторонняя аутентификация

- односторонняя: клиент доказывает свою подлинность серверу. Здесь примером может служить процедура входа пользователя в систему
- двусторонняя: обе стороны подтверждают свою подлинность. Примером такой аутентификации является защищённое соединение по протоколу HTTPS, которое используется для веб-сайтов. Например, когда пользователь вводит свои логин и пароль на сайте како-нибудь банка, а сайт в ответ предоставляет пользователю цифровой сертификат, который подтверждает, что этот сайт подлинный и действительно принадлежит тому, за кого себя выдает.Это позволяет защититься от подмены сайта для кражи данных [3].

2. Одно-, двух- и трёхфакторная аутентификация

- однофакторная - требует подтверждения только одним способом — например, с помощью пароля. Она встречается чаще всего.
- двухфакторная - требует от пользователя подтверждения двумя способами аутентификации сразу. Например, при входе в соцсеть у пользователя могут попросить не только пароль, но и другую информацию — код из СМС или биометрические данные. Используется в системах, в которых хранятся

какие-то важные личные данные. Знакомым для нас примером является Github, где можно подключить двухфаткорную аутентификацию. Тогда при входе нужно будет ввести не только пароль, но и код из специального приложения, который постоянно обновляется

- трехфакторная - встречается значительно реже, обычно в системах с повышенными требованиями к безопасности. Такая аутентификация требует трех методов: например, пароль + код из СМС + отпечаток пальца [4].

Для проведения процедур идентификации и аутентификации пользователя необходимы:

- наличие соответствующего субъекта (модуля) аутентификации - программное или аппаратное средство, которое обрабатывает запросы на аутентификацию, сравнивая предоставленные пользователем данные с хранящимися в системе.
- наличие аутентифицирующего объекта, хранящего уникальную информацию для аутентификации пользователя

Различают две формы представления объектов, аутентифицирующих пользователя:

- внешний аутентифицирующий объект, не принадлежащий системе- Примеры включают: аппаратные токены (например, USB-ключи), смарт-карты, внешние устройства для генерации одноразовых паролей (OTP).
- внутренний объект, принадлежащий системе, в который переносится информация из внешнего объекта. Например: база данных пользователей с хранящимися паролями или биометрическими шаблонами или системы хранения данных о токенах и других средствах аутентификации [5].

Как эти понятия связаны между собой? На самом деле, эти процессы происходят последовательно, друг за другом, и завершается все процессом авторизации,

который мы не затронули в данной докалде. Посмотрим на такую последовательность на примере из повседневной жизни: заход на свой почтовый ящик.

1) Идентификация: определение личности пользователя. В нашем случае, ввод адреса электронной посты (логин)
2) Аутентификация: проверка подлинности. Это ввод пароля.
3) Авторизация: предоставление прав доступа к ресурсам. Здесь возможность читать, отправлять и удалять письма

4.1 Типовая схема идентификации и аутентфиикации

Рассмотрим модифицированную схему индентификации и аутентификации. Допустим, что в компьютерной системе зарегистрировано n пользователей. Пусть i-й аутентифицирующий объект i-го пользователя содержит два информационных поля:

- IDi- неизменный идентификатор i-го пользователя, который является аналогом имени и используется для идентификации пользователя
- Ki - аутентифицирующая информация пользователя, которая может изменяться и служит для аутентификации (например, пароль $i = i$).

В компьютерной системе выделяется модифицированный объект-эталон, структура которого показана в табл. 4.1. В нем значение E_i равно $F(S_iK_i)$, где S_i случайный вектор, задаваемый при создании идентификатора пользователя, т.е. при создании строки, необходимой для идентификации и аутентификации пользователя; F-функция, которая обладает свойством “невосстановимости” значения K_i по E_i и S_i.

Таблица 4.1: Модифицированный объект-эталон

Номер пользователя	Информация для идентификации	Информация для аутентификации
1	ID_1	E_1
2	ID_2	E_1
...	...	...
N	ID_i	E_i

Протокол идентификации и аутентификации для нашей схемы выглядит следующим образом:

1. Пользователь предъявляет свой идентификатор ID.
2. Если ID не совпадает ни с одним ID_i, зарегистрированным в компьютерной системе, то идентификация отвергается - пользователь не допускается к работе, иначе (существует IDi=ID) устанавливается, что пользователь, называвшийся пользователем i, прошел идентификацию.
3. По идентификатору ID_i выделяется вектор S_i.
4. Субъект аутентификации запрашивает у пользователя аутентификатор K.
5. Субъект аутентификации вычисляет значение $Y = F(S_i, K)$.
6. Субъект аутентификации производит сравнение значений Y и E_i. При совпадении этих значений устанавливается, что данный пользователь успешно аутентифицирован в системе. В противном случае аутентификация отвергается - пользователь не допускается к работе.

Такая схема аутентификации применяется в ОС UNIX. В качестве идентификатора ID используется имя пользователя (запрошенное по Loqin), в качестве аутентификатора K_i - пароль пользователя (запрошенный по Password), функция

F представляет собой алгоритм шифрования DES. Эталоны для идентификации и аутентификации содержатся в файле Etc/passwd [5].

4.2 Популярные способы аутентификации:

Рассмотрим наиболее поппулярные способы аутентификации:

1) Парольная аутентификация

Главное достоинство парольной аутентификации - простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности, однако по совокупности характеристик их следует признать самым слабым средством проверки подлинности, так как они зачастую просты для запоминаия, стандартны и их легко подобрать или подсмотреть [3].

Простейший метод подтверждения подлинности с использованием пароля основан на сравнении представляемого пользователем пароля P_A. С исходным значением $P_{A'}$, хранящимся в компьютерном центре. Поскольку пароль должен храниться в тайне, он должен шифроваться перед пересылкой по незащищенному каналу. Если значения P_A и $P_{A'}$ совпадают, то пароль P_A считается подлинным, а пользователь - законным (рис. 4.3) [5].

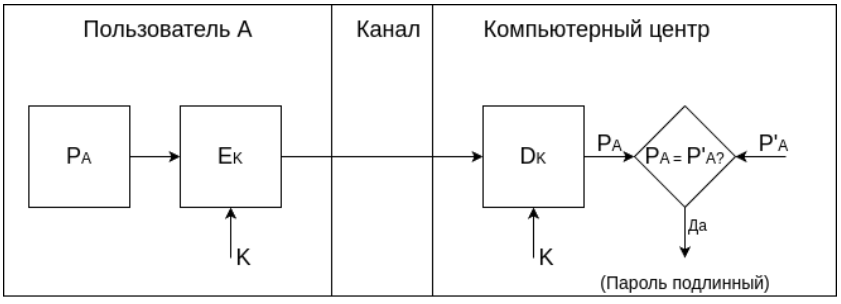

Рис. 4.3: Схема простой аутентификации с помощью пароля

2) Биометрическая аутентификация

Биометрия представляет собой совокупность автоматизированных методов идентификации и/или аутентификации людей на основе их физиологических и поведенческих характеристик. К числу физиологических характеристик принадлежат особенности отпечатков пальцев, сетчатки и роговицы глаз, геометрия руки и лица и т.п. К поведенческим характеристикам относятся динамика подписи (ручной), стиль работы с клавиатурой. На стыке физиологии и поведения находятся анализ особенностей голоса и распознавание речи.

В общем виде работа с биометрическими данными организована следующим образом. Сначала создается и поддерживается база данных характеристик потенциальных пользователей. Для этого биометрические характеристики пользователя снимаются, обрабатываются, и результат обработки, называемый биометрическим шаблоном, заносится в базу данных.В дальнейшем для идентификации (и одновременно аутентификации) пользователя процесс снятия и обработки повторяется, после чего производится поиск в базе данных шаблонов. В случае успешного поиска личность пользователя и ее подлинность считаются установленными. Для аутентификации достаточно произвести сравнение с одним биометрическим шаблоном, выбранным на основе предварительно введенных данных [3].

5 Управление доступом

Управление доступом является важным компонентом информационной безопасности, обеспечивая контроль за тем, кто и как может взаимодействовать с информационными ресурсами организации. Эффективное управление доступом помогает предотвратить несанкционированный доступ и защитить конфиденциальную информацию.

Управление доступом включает в себя несколько основных задач:

- Определение объектов доступа: это могут быть информационные системы, базы данных и другие ресурсы, к которым требуется контроль доступа.
- Идентификация субъектов доступа: учетные записи пользователей, аккаунты в облачных сервисах и другие идентификаторы.
- Разработка матрицы доступа: правила разграничения доступа, определяющие, кто и какие права имеет на доступ к конкретным ресурсам. Обычно эти отношение “объект-субъект” можно представить в виде матрицы доступа, которая вглядит следующим образом 5.1. В строках которой перечислены субъекты, в столбцах - объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия (например, время и место действия) и разрешенные виды доступа. Права доустпа обозначаются следующим образом: “o” - разрешение на передачу прав доступа другим пользователям, “r” - чтение, “w” - запись, “e” - выполнение, “a” - добавление информации [3].

Таблица 5.1: Матрица доступа

Сбуъекты/Объекты	Файл	Программа	Линия связи	Базад данных
User 1	r	rwe	rw с 9:00 до 18:00	rw
User 2	rw	r	orw	
User 3	rwo	rw		r

- Управление учетными записями: создание, изменение, удаление и блокировка учетных записей пользователей.
- Аудит прав доступа: регулярная проверка предоставленных прав для выявления избыточных или неиспользуемых учетных записей.

5.1 Модели и технологии управления доступом

Существует несколько моделей управления доступом, каждая из которых имеет свои особенности и применение:

1) Дискреционная модель управления доступом (DAC):

В этой модели владелец объекта сам может устанавливать и изменять права доступа к объекту. Это дает гибкость, но также может привести к рискам безопасности, если права не контролируются должным образом. Хорошим примером такой модели являются операционные системы (Windows, UNIX)

2) Мандатная модель управления доступом (MAC): Доступ определяется на основе меток конфиденциальности. Пользователи могут получать доступ только к тем объектам, уровень безопасности которых соответствует их уровню допуска. Эта модель обеспечивает более строгий контроль и защиту от утечек информации. Часто используется в военных и правительственных организациях.

3) Ролевая модель управления доступом (RBAC): Права доступа назначаются ролям (например, “Администратор”, “Пользователь”, “Гость”), а не отдельным пользователям, причем эти роли могут быть иерархическими. Это упрощает администрирование, так как нужно назначать права досутпа ролям, а не каждому пользователю. Такая модель позволяет реализовать статическое и динамическое разделение полномочий. Очень популярно в крупных организациях.

4) Модель управления доступом на основании правил (RuBAC): Доступ предоставляется на основе логических правил «если-то», заданных администратором. Например: размер документа не больше 5Мб, доступ только в будние дни в рабочее время и для сотрудников с формой допуска №3.Это позволяет гибко управлять правами доступа в зависимости от условий [6].

Современные системы управления доступом могут включать различные технологии:

1) Логические системы: обеспечивают контроль доступа к информационным системам с помощью паролей, двухфакторной аутентификации и шифрования.
2) Физические системы: используют электронные ключи, биометрические системы и камеры для контроля доступа к физическим объектам.
3) Сетевые системы: управляют доступом к сетевым ресурсам и обеспечивают авторизацию пользователей.

6 Выводы

В данном докладе были рассмотрены ключевые понятия идентификации и аутентификации, их классификация и типовые схемы. Мы кратко описали два популярных метода аутентификации и изучили задачи управления доступом, а также распространенные модели и технологии. Понимание этих процессов является важным шагом к обеспечению безопасности информации и ресурсов в современных организациях.

Список литературы

1. Лекция 33-34 «Идентификация и аутентификация. Управление доступом» [Электронный ресурс]. Российский государственный педагогический университет им. А.И. Герцена, 2018. URL: https://studfile.net/preview/7365983/page:16/.
2. Многофакторная аутентификация [Электронный ресурс]. Wikimedia Foundation, Inc., 2023. URL: https://ru.wikipedia.org/wiki/Многофакторная_аутентификация/.
3. Идентификация и аутентификация, управление доступом [Электронный ресурс]. Интернет Университет Информационных Технологий, 2006. URL: https://citforum.ru/security/articles/galatenko/.
4. Идентификация, аутентификация, авторизация: чем они различаются [Электронный ресурс]. Skillbox, 2023. URL: https://skillbox.ru/media/code/identifikatsiya-autentifikatsiya-avtorizatsiya-chem-oni-razlichayutsya/.
5. С. К. Варлатая М.В.Ш. Аппаратно-программные средства и методы защиты информации. Владивосток: ДВГТУ, 2007. 318 с.
6. Управление доступом и учетными записями [Электронный ресурс]. Интеллектуальная безопасность» (Security Vision), 2020. URL: https://www.securityvision.ru/blog/avtomatizatsiya-protsessov-upravleniya-informatsionnoy-bezopasnostyu-upravlenie-dostupom-i-uchetnymi/.