МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ   
ФГАОУ ВО «СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»   
ФАКУЛЬТЕТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК ИМЕНИ ПРОФЕССОРА Н. И. ЧЕРВЯКОВА

КАФЕДРА ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И КИБЕРНЕТИКИ

**ОТЧЁТ**

**«НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА»**

**Выполнил:**

студент 4 курса

группы ИБАС-с-о-21-1 специальности 10.05.03  
«Информационная безопасность  
автоматизированных систем»  
очной формы обучения

Новиков Кирилл Игоревич

(подпись)

**Руководитель практики:**

Доцент кафедры вычислительной математики и кибернетики  
Пелешенко Татьяна Александровна

(подпись)

Ставрополь, 2025

Содержание

[Введение 3](#_Toc208608729)

[1. Аутентификация в автоматизированных системах 4](#_Toc208608730)

[2. Управление доступом в автоматизированных системах 6](#_Toc208608731)

[3. Простые методы защиты критических узлов 9](#_Toc208608732)

[4. Практическая значимость применения аутентификации и управления доступом в АС 12](#_Toc208608733)

[Заключение 14](#_Toc208608734)

[Список литературы 16](#_Toc208608735)

# 

# Введение

Современные автоматизированные системы (АС) становятся все более сложными и взаимосвязанными, что повышает их уязвимость к несанкционированному доступу и кибератакам. Нарушение работы критических узлов таких систем может привести к сбоям технологических процессов, утечке конфиденциальной информации и значительным финансовым потерям. Поэтому вопросы аутентификации и управления доступом занимают ключевое место в обеспечении информационной безопасности АС.

Аутентификация служит первым рубежом защиты, подтверждая личность пользователя или устройства, а управление доступом регулирует их действия в пределах системы. Даже простые методы — логины и пароли, уровни прав доступа, регулярная смена учетных данных — значительно снижают риск инцидентов безопасности.

Целью настоящей статьи является исследование роли аутентификации и управления доступом в автоматизированных системах, анализ их практической значимости и рассмотрение простых, но эффективных методов защиты критических узлов. В рамках исследования ставятся задачи описания существующих подходов к аутентификации, классификации методов управления доступом, а также формулирования рекомендаций по их применению для повышения уровня защищенности АС.

### ****1. Аутентификация в автоматизированных системах****

Аутентификация — это процесс проверки подлинности пользователя, устройства или программы, которые пытаются получить доступ к системе. В АС она выполняет ключевую роль, так как позволяет не допустить случайного или злонамеренного вмешательства в управление технологическими процессами.

#### ****1.1 Классические методы аутентификации****

1. **Логин и пароль**  
   Самый распространенный способ, при котором пользователь вводит идентификатор (логин) и секрет (пароль).
   * **Преимущества:** простота реализации, поддерживается всеми системами.
   * **Недостатки:** пароли часто подбираются злоумышленниками методом перебора, фишинга или утечек.
   * **Рекомендации:** использование паролей длиной не менее 10–12 символов, обязательное присутствие букв разных регистров, цифр и спецсимволов, регулярная смена паролей (раз в 60–90 дней).
2. **Одноразовые пароли (OTP)**  
   OTP генерируются приложением (Google Authenticator) или аппаратным токеном и действуют ограниченное время (30–60 секунд).
   * **Применение в АС:** удобно для операторов, которые редко подключаются к удалённым узлам.
   * **Плюсы:** защита от кражи пароля, бесполезность старого кода.
   * **Минусы:** необходимость доступа к токену или телефону.
3. **Смарт-карты и токены**  
   Используются в корпоративных АС и SCADA-системах. Смарт-карта хранит криптографический ключ, который подтверждает личность пользователя.
   * **Применение:** безопасный вход на рабочие станции операторов.
   * **Преимущество:** сложно подделать, можно отозвать ключ при увольнении сотрудника.

#### ****1.2 Многофакторная аутентификация (MFA)****

MFA требует комбинации факторов:

* **Знание** (пароль),
* **Владение** (смарт-карта, токен),
* **Биометрия** (отпечаток пальца, скан лица).

В АС особенно важен второй фактор, так как пароли операторов могут храниться на бумаге рядом с пультом (что является частой практикой на старых объектах). MFA уменьшает риск, что злоумышленник, получивший пароль, сможет получить доступ к системе.

#### ****1.3 Проблемы и угрозы аутентификации****

* **Социальная инженерия:** злоумышленники могут выманивать пароли, представляясь службой поддержки.
* **Повторное использование паролей:** если пароль совпадает с корпоративной почтой, его утечка с внешнего сайта даст злоумышленнику доступ к АС.
* **Слабые политики смены паролей:** редко меняемые пароли или стандартные комбинации (admin/admin) открывают прямую дорогу атакующему.

### ****2. Управление доступом в автоматизированных системах****

Управление доступом — это процесс, который определяет, какие действия могут выполнять пользователи или устройства в системе. Если аутентификация отвечает на вопрос «кто вы?», то управление доступом отвечает на вопрос «что вы можете делать?».

В автоматизированных системах, особенно там, где присутствуют критические узлы управления (SCADA, PLC, HMI), корректная настройка прав доступа жизненно важна. Ошибки в этой области могут привести к саботажу, случайным остановкам производственного процесса или утечкам конфиденциальных данных.

#### ****2.1 Основные модели управления доступом****

Существует несколько подходов к организации контроля доступа. Наиболее распространенные:

1. **DAC (Discretionary Access Control)** — дискреционный контроль доступа
   * **Принцип:** владелец ресурса (файл, база данных, контроллер) сам определяет, кто и что может с ним делать.
   * **Пример:** оператор технологического участка может дать коллеге доступ к файлу отчета без участия администратора.
   * **Плюсы:** гибкость, простота реализации.
   * **Минусы:** риск ошибок — владелец может случайно дать лишние права.
2. **MAC (Mandatory Access Control)** — мандатный контроль доступа
   * **Принцип:** правила доступа определяются администратором системы и не могут изменяться пользователями.
   * **Пример:** в системе управления электроподстанцией все объекты имеют метки безопасности («Секретно», «Конфиденциально»), и только определенные роли могут их изменять.
   * **Плюсы:** высокая защищенность, строгие правила.
   * **Минусы:** меньшая гибкость, сложность администрирования.
3. **RBAC (Role-Based Access Control)** — ролевой контроль доступа
   * **Принцип:** каждому пользователю назначается роль (оператор, инженер, администратор), а роли уже привязаны к определенным правам.
   * **Пример:** роль «Оператор» может запускать и останавливать технологические процессы, но не изменять конфигурацию оборудования.
   * **Плюсы:** масштабируемость — при появлении нового сотрудника ему достаточно назначить роль.
   * **Минусы:** сложность проектирования при большом количестве ролей.

#### ****2.2 Сравнение моделей управления доступом****

| **Модель** | **Гибкость** | **Безопасность** | **Управляемость** | **Где применяется** |
| --- | --- | --- | --- | --- |
| DAC | Высокая | Средняя | Простая | Локальные сети, небольшие АС |
| MAC | Низкая | Очень высокая | Сложная | Военные системы, критическая инфраструктура |
| RBAC | Средняя | Высокая | Удобная при масштабировании | Крупные промышленные АС |

#### ****2.3 Принципы построения системы управления доступом****

* **Принцип наименьших привилегий:** каждый пользователь получает только те права, которые необходимы для выполнения его работы.
* **Разделение обязанностей:** критические действия (например, внесение изменений в систему управления) должны требовать подтверждения двух разных ролей (оператор + инженер).
* **Регулярный аудит прав:** хотя бы раз в квартал необходимо проверять, нет ли у сотрудников лишних или неиспользуемых прав.
* **Ведение логов:** каждая попытка входа и каждое изменение прав должны фиксироваться и анализироваться.

#### ****2.4 Угрозы, связанные с управлением доступом****

1. **Эскалация привилегий:** злоумышленник получает более высокий уровень доступа, чем ему положено, например, за счет уязвимости в системе.
2. **Неправильная конфигурация:** администратор случайно оставил гостевой доступ или выдал слишком широкие права.
3. **Отсутствие актуализации прав:** уволенный сотрудник продолжает иметь доступ к системе.

Пример из практики: на одном из промышленных предприятий после увольнения инженера его учетная запись осталась активной еще 3 месяца, и он мог удаленно подключаться к системе SCADA. Это создавало риск несанкционированного вмешательства в управление производством.

### ****3. Простые методы защиты критических узлов****

Даже в тех автоматизированных системах (АС), где нет сложных и дорогих решений класса IDS/IPS, можно значительно снизить риски при помощи простых организационных и технических мер.

#### ****3.1 Разделение прав и сегментация сети****

Одной из ключевых угроз для АС является распространение инцидента на всю сеть — если злоумышленник получил доступ к одной станции, он может атаковать соседние узлы. Для снижения этого риска используется сегментация:

* **Выделение отдельных VLAN для разных уровней АС:**
  + Уровень операторских станций (HMI)
  + Уровень контроллеров (PLC)
  + Уровень корпоративных систем (ERP, CRM)
* **Ограничение маршрутизации между сегментами:** например, SCADA-сеть не должна быть напрямую доступна с компьютеров бухгалтерии.
* **Использование межсетевых экранов (firewall):** фильтрация трафика между сегментами, разрешение только необходимых протоколов (Modbus, OPC UA).

Пример: на одном производстве внедрение VLAN и простого L3-файрвола снизило количество инцидентов с вирусами на операторских станциях на 70%, так как зараженные компьютеры из офиса перестали иметь доступ к SCADA.

#### ****3.2 Аутентификация и защита паролей****

Даже самая простая система должна требовать от пользователей уникальные учетные записи. Практические рекомендации:

* Использовать **уникальные логины** для каждого сотрудника, запретив учетные записи «admin/admin» или «operator/operator».
* Настроить **политику сложности паролей**: не менее 8 символов, наличие букв и цифр, запрет на пароли из «черных списков» (123456, qwerty).
* **Регулярная смена паролей** — хотя бы раз в 90 дней для критических ролей (администратор, инженер).
* Хранение паролей в хэшированном виде (bcrypt, scrypt) — это актуально даже для локальных SCADA-систем.

#### ****3.3 Логирование и мониторинг****

Логи — это «черный ящик» безопасности. Даже если атака произошла, по логам можно определить, кто и когда получил доступ.

* Включить логирование на всех серверах, HMI и контроллерах, где это возможно.
* Настроить централизованный сбор логов (например, на syslog-сервер).
* Внедрить простейшие правила корреляции — например, уведомлять администратора, если:
  + более 3 неудачных попыток входа с одной учетной записи за 5 минут;
  + вход в систему производится в нерабочее время (ночью).

#### ****3.4 Резервное копирование и откат системы****

Даже простое резервное копирование конфигураций и баз данных помогает восстановить систему после атаки или поломки.

* Хранить бэкапы на изолированных носителях (NAS с отдельной учеткой или съемные диски).
* Проверять восстановление — хотя бы раз в квартал тестировать, что бэкап действительно можно развернуть.
* Создавать резервные образы HMI-станций — это ускоряет восстановление работы после вирусных заражений.

#### ****3.5 Типичные атаки и как их предотвратить простыми средствами****

1. **Stuxnet (2010):** вредонос заражал USB-накопители, через которые попадал в изолированные сети.
   * **Простая мера защиты:** запрет использования внешних флешек, контроль USB-портов через Group Policy.
2. **BlackEnergy (2015):** атака на энергосистему Украины, использовались фишинговые письма и удаленный доступ к SCADA.
   * **Простая мера защиты:** двухфакторная аутентификация для удаленных VPN, обучение сотрудников распознаванию фишинга.
3. **Внутренние угрозы:** сотрудник с доступом может случайно или намеренно изменить настройки оборудования.
   * **Простая мера защиты:** принцип «двух ключей» — критические команды требуют подтверждения двумя пользователями.

#### ****3.6 Организационные меры****

Технические средства — это половина успеха. Не менее важны организационные меры:

* Проведение регулярных инструктажей и мини-тренингов для операторов.
* Создание простых инструкций — что делать при сбое, вирусной атаке, подозрительном поведении системы.
* Наличие назначенного ответственного за ИБ даже в малых предприятиях.

### ****4. Практическая значимость применения аутентификации и управления доступом в АС****

Внедрение даже простейших мер по аутентификации и разграничению прав доступа существенно повышает киберустойчивость автоматизированных систем. В условиях ограниченного бюджета, особенно на малых и средних предприятиях, где нет возможности развернуть SIEM, SOC или коммерческие IDS/IPS, базовые механизмы защиты играют ключевую роль.

#### ****4.1 Снижение вероятности инцидентов****

Исследования показывают, что до 80% инцидентов ИБ в АС происходят из-за ошибок персонала или слабых паролей. Если внедрить политику сложных паролей и уникальных логинов, можно снизить вероятность успешного подбора учетных данных в несколько раз.

* **Пример расчета:**
  + Базовый пароль: «12345» — перебирается за миллисекунды.
  + Пароль из 10 случайных символов (буквы+цифры): перебор на обычном ПК займет месяцы.
  + Если добавить двухфакторную аутентификацию — вероятность взлома учетной записи становится практически нулевой.

#### ****4.2 Сокращение времени реакции на инциденты****

Логирование и централизованный мониторинг помогают быстрее выявлять проблемы.  
Без логов расследование атаки может занять **дни**, а с журналами событий — **часы**.  
Например, при заражении станции вирусом можно быстро определить, с какого USB-накопителя произошло заражение, и локализовать проблему, не отключая всю систему.

#### ****4.3 Экономический эффект****

Простые меры стоят дешевле, чем последствия киберинцидента:

| **Мера** | **Стоимость внедрения** | **Потенциальный эффект** |
| --- | --- | --- |
| Введение политики сложных паролей | ≈0 (только настройка в ОС) | Снижение риска брутфорса на 70–90% |
| Разделение VLAN и установка простого L3-файрвола | 50000–100000 рублей | Снижение риска распространения вирусов и червей |
| Логирование и сбор событий на syslog | бесплатно (встроенные средства) | Сокращение времени расследования инцидента в 3–5 раз |
| Обучение персонала 1 раз в квартал | 10000–20000 рублей | Снижение числа фишинг-инцидентов до 50% |

Даже минимальные вложения дают диспропорционально высокий результат — особенно в системах, где простой оборудования обходится в тысячи рублей за час.

#### ****4.4 Повышение доверия заказчиков и регуляторов****

Для предприятий, работающих с критической инфраструктурой, выполнение минимальных требований по ИБ является обязательным (например, ФЗ-187 в РФ или NIS2 в ЕС). Наличие аутентификации, управления доступом и журналирования событий позволяет пройти аудит и избежать штрафов.

#### ****4.5 Пример из практики****

На одном пищевом производстве операторская станция SCADA несколько раз заражалась вирусами через USB-флешки подрядчиков. После внедрения простого контроля устройств (разрешены только подписанные флешки), а также раздельных учетных записей для операторов и подрядчиков, количество инцидентов снизилось с 4-5 в год до **0**.  
Стоимость решения составила менее 15 000 рублей, а эффект — отсутствие простоя оборудования (каждый простой обходился предприятию в ≈1 000 000 рублей).

### ****Заключение****

Проведенный анализ показал, что аутентификация и управление доступом являются краеугольными камнями безопасности автоматизированных систем. Именно эти механизмы позволяют ограничивать действия пользователей, защищать критические узлы от несанкционированного вмешательства и предотвращать распространение атак внутри сети.

Даже базовые меры — уникальные логины, политика сложных паролей, двухфакторная аутентификация, сегментация сети и журналирование событий — способны значительно снизить риск инцидентов, сократить время реакции на сбои и повысить надежность работы всей системы.  
Эти меры особенно актуальны для малых и средних предприятий, которые не имеют возможности внедрять дорогостоящие средства класса SIEM или корпоративные SOC.

В ходе работы были рассмотрены:

* современные подходы к аутентификации (парольная, токеновая, биометрическая, многофакторная);
* модели управления доступом (DAC, MAC, RBAC) и их применение в АС;
* практические рекомендации по защите критических узлов с учетом ограниченных ресурсов;
* примеры успешного снижения риска на предприятиях с помощью простых организационно-технических мер.

Результаты исследования подтверждают, что даже при минимальных вложениях в защиту можно существенно повысить киберустойчивость АС и соответствовать требованиям нормативных документов.  
Применение предложенных мер снижает вероятность простоев, утечек данных и аварий, а также укрепляет доверие клиентов, партнеров и регуляторов.

Таким образом, внедрение базовых мер аутентификации и управления доступом следует рассматривать как обязательный первый шаг на пути построения комплексной системы информационной безопасности на любом предприятии.

### ****Список литературы****

1. ГОСТ Р 56939-2016 «Защита информации. Информационные технологии. Процессы жизненного цикла автоматизированных систем»
2. ISO/IEC 27001:2022 «Information security, cybersecurity and privacy protection — Information security management systems»
3. NIST SP 800-53 Rev.5 «Security and Privacy Controls for Information Systems and Organizations»
4. Н. Я. Матросов, В. В. Степанов. «Информационная безопасность автоматизированных систем». Учебное пособие. — М.: БХВ-Петербург, 2020.
5. С. С. Петров. «Практическая защита АСУ ТП». — СПб.: Питер, 2021.
6. OWASP Cheat Sheets — Authentication, Access Control. https://cheatsheetseries.owasp.org
7. ENISA. «Good Practices for Security of Smart Manufacturing». — European Union Agency for Cybersecurity, 2022.