**РадиоХак 2.0 2025 | ИРИТ-РТФ | Прософт-Системы**

**РадиоХак 2.0** – это соревнование, где студенческие команды решают практические задачи от компаний-партнёров. Участники создают прототипы решений за ограниченное время, а лучшие проекты получают призы.

**Название:** Разработка сервиса централизованной авторизации для промышленных контроллеров в электроэнергетике.

**Краткое описание кейса:** Создание MVP-сервиса централизованной авторизации, который заменит разрозненные системы хранения учетных данных на промышленных контроллерах. Сервис обеспечит единый, безопасный и управляемый доступ к контроллерам, упростит администрирование пользователей и повысит общую безопасность объектов электроэнергетики.

**Даты проведения:**

– 6 октября 10:00 старт хакатона

– 6-8 октября дни работы в формате онлайн

– 8 октября 18:00 СТОП-КОД, сдача

– 8-9 октября проверка работ

– Дата очного награждения будет объявлена 6 октября

**Призовой фонд на трек:**

1 место: 30.000р. на команду

2 место: 20.000р. на команду

3 место: 10.000р. на команду

**Постановка задачи**

Необходимо разработать прототип приложения — сервер авторизации, который будет выполнять следующие функции:

1. **Хранение учетных данных пользователей** — в энергонезависимой памяти (файл JSON/XML/YAML или база данных).
2. **Идентификация и аутентификация** — при запуске приложение запрашивает логин и пароль, проверяет их наличие и корректность.
3. **Автоматическое создание администратора** — если учетная запись admin отсутствует, приложение создаёт её с паролем по умолчанию.
4. **Принудительная смена пароля администратора** — после первого входа с паролем по умолчанию, система требует его замены.
5. **Авторизация администратора** — предоставляет права на просмотр списка пользователей, создание и удаление учетных записей.
6. **Безопасное хранение паролей** — рекомендуется хранить пароли в виде хешей.
7. **Интерфейс пользователя** — допускается CLI, GUI или оба варианта на выбор команды.

**Технические требования:**

Техническая часть должна быть реализована на С++.

**Проблематика:**

Сегодня на объектах электроэнергетики каждый контроллер хранит учетные записи пользователей локально. Это приводит к следующим проблемам:

**Отсутствие централизованного управления** — администратор вынужден вручную синхронизировать учетные данные на каждом устройстве.

**Риск рассинхронизации и ошибок** — при изменении прав или удалении пользователя легко пропустить один из контроллеров.

**Снижение уровня безопасности** — устаревшие или дублирующиеся учетные записи остаются активными, а пароли часто хранятся в открытом виде.

**Сложность аудита** — невозможно отследить, кто, когда и на каком устройстве получил доступ.

Решение:

Разработанный сервис авторизации:

**Централизует управление доступом** — все учетные данные хранятся в одном месте, что упрощает администрирование и аудит.

**Автоматизирует процессы** — создание, удаление и изменение учетных записей происходит через единый интерфейс.

**Повышает безопасность** — рекомендуется хеширование паролей, обязательная смена пароля по умолчанию, контроль доступа по ролям.

**Формат сдачи работ:**Для сдачи своих проектов необходимо заполнить форму **до 8 октября (18:00)**, в которую необходимо загрузить ссылки на git, презентацию.

Форма сбора ответов будет направлена 8 октября.

**Оценка**

***Отраслевые критерии:***

**01. Релевантность поставленной задаче (0–3 балла):**

o Команда продемонстрировала понимание проблематики.

o Предложенное решение полностью соответствует поставленной задаче.

**02. Проработка пользовательских сценариев (UX/UI) (0–3 балла):**

o Интерфейс (CLI/GUI) интуитивно понятен для технических пользователей.

o Реализованы ключевые сценарии: вход, смена пароля, управление пользователями.

**03. Реализация ключевых требований Заказчика (0–3 балла):**

o Корректно реализованы идентификация, аутентификация и авторизация.

o Обязательная смена пароля администратора после первого входа.

o Поддержка хранения данных в энергонезависимой памяти(БД).

**04. Демонстрация решения (0–3 балла):**

o Презентация логична, охватывает архитектуру, безопасность и UX.

o Плюс за работающий прототип, который можно запустить и протестировать на месте.

***Технические критерии:***

**01. Качество и чистота кода (0–6 баллов):**

o Код структурирован, модульный, с комментариями и понятной логикой.

o Четко разделены слои: аутентификация, авторизация, хранилище, интерфейс.

o Наличие README с инструкцией по установке, запуску и тестированию.

**02. Безопасность (0–3 балла):**

o Пароли хранятся в хешированном виде.

o Реализована защита от перебора (rate limiting, блокировка после N попыток — если реализовано).

o Учетные данные не выводятся в логи в открытом виде.

**03. Докеризация (0–1 балл):**

o Приложение упаковано в Docker-контейнер для быстрого развертывания и тестирования.

**04. Реализация дополнительного задания (0–5 баллов):**

o Поддержка аудита — логирование всех действий администратора.

o Возможность импорта/экспорта базы пользователей.

**05. Защита команды (0–3 балла):**

o Команда уверенно отвечает на вопросы по архитектуре, безопасности и масштабируемости.

o Готова обосновать выбор технологий и подходов.

## Участники могут:

* Критиковать любое представление в уважительной манере.
* Сделать видео или любую публикацию в социальных сетях об этом хакатоне в уважительной форме.
* Выдвигать предложения или сообщать о любых неудобствах в уважительной форме.

## Организаторы имеют право:

* дисквалифицировать команды без предупреждения и объяснения причин.
* решение жюри и организаторов обжалованию не подлежит.
* вносить изменения в правила и положения, предварительно проинформировав участников через организаторов со стороны УрФУ.

**Примечание:**

Компания-партнёр хакатона получает неисключительное, безвозмездное, бессрочное и безотзывное право на использование всех материалов, созданных участниками в рамках выполнения кейса (включая, но не ограничиваясь: исходный код, документацию, презентации, видеоматериалы, дизайн-макеты и иные результаты интеллектуальной деятельности), в любых целях, в том числе для коммерческого использования, без дополнительного согласования с участниками и без выплаты вознаграждения. Участники подтверждают, что предоставляемые материалы не нарушают прав третьих лиц.