Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет ИТМО»

Факультет программной инженерии и компьютерной техники

Вопрос-ответ

«Учетные записи и авторизация в ОС MS Windows»

по дисциплине

«Информационная безопасность»

Вариант № 49

Группа: P34102

Выполнил: Лапин А.А.

Проверил:
Рыбаков С.Д.

Санкт-Петербург
2024г.

Оглавление

Есть админ и пользователь. Что будет, если попробовать разными способыми убрать админу админа? Кто будет админом или так нельзя?

Можно удалить всех админов из системы, тогда вы не сможете управлять многими системными настройками и устанавливать программы. В таком случае для восстановления работоспособности потребуется создание нового администратора через безопасный режим или восстановление системы.

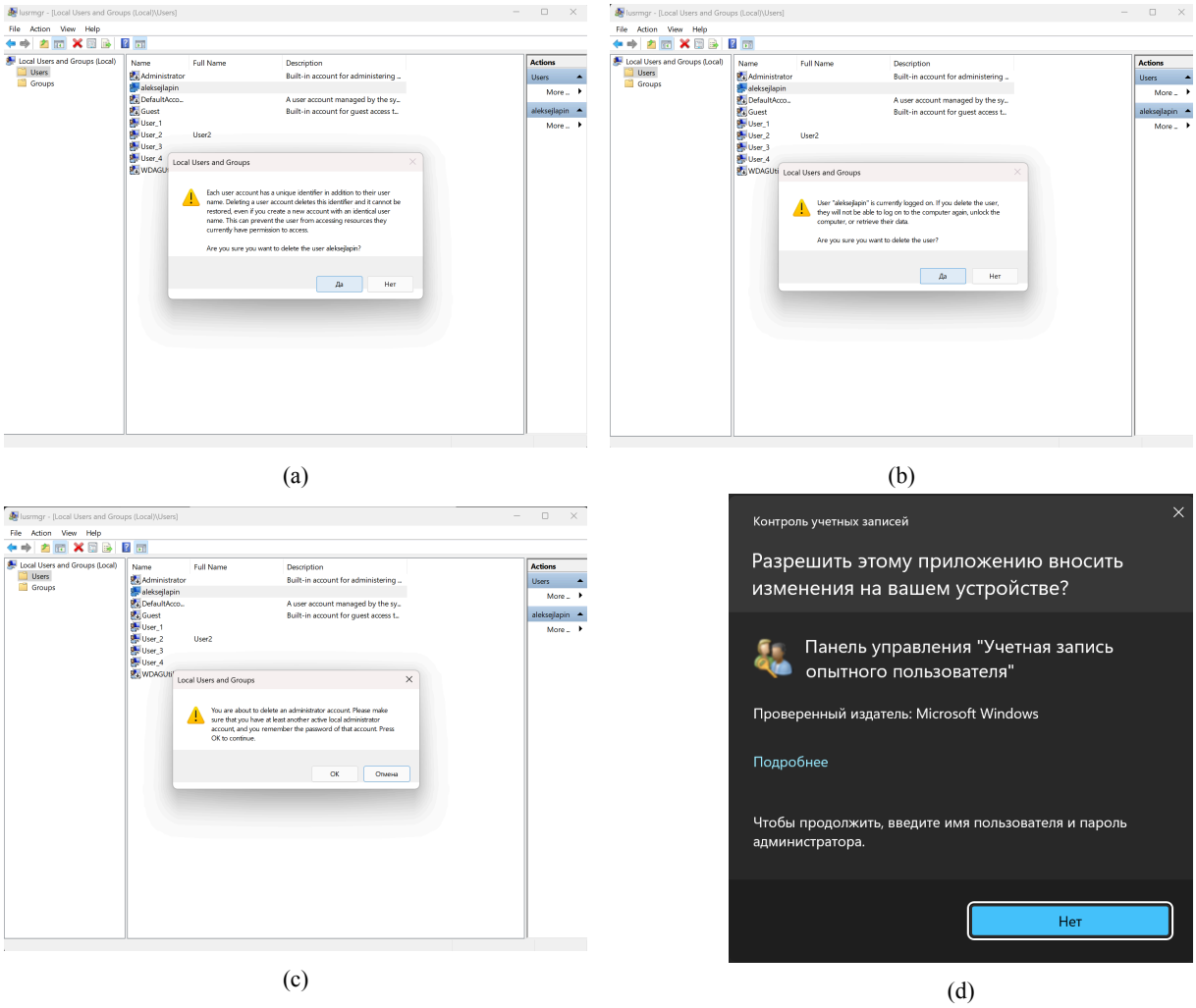

Рис. 1: Результаты работы программы

Кто такие КИИ? Как понять, относитесь вы к ним или нет?

Определения

Критическая информационная инфраструктура (сокращенно - КИИ) – это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ, а также сети электросвязи, используемые для организации их взаимодействия.

Субъекты КИИ – это компании, работающие в стратегически важных для государства областях, таких как здравоохранение, наука, транспорт, связь, энергетика, банковская сфера, топливно-энергетический комплекс, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, а также организации, обеспечивающие взаимодействие систем или сетей КИИ.

Категория значимости объекта КИИ может принимать одно из трех значений (где самая высокая категория - первая, самая низкая - третья) и зависит от количественных показателей значимости этого объекта в социальной, политической, экономической и оборонной сферах. Например, если компьютерный инцидент на объекте КИИ может привести к причинению ущерба жизни и здоровью более 500 граждан, то объекту присваивается максимальная первая категория, а если услуги связи в результате инцидента КИИ могут стать недоступны для 3 тыс. - 1 млн. абонентов, то объекту присваивается минимальная третья категория.

В России понятие КИИ регулируется **Федеральным законом №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»**, вступившим в силу 1 января 2018 года. Этот закон определяет основные принципы защиты КИИ и устанавливает ответственность за обеспечение их безопасности[2].

1 Основные элементы КИИ

- **Объекты КИИ:**
  - Информационные системы.
  - Информационно-телекоммуникационные сети.
  - Автоматизированные системы управления.
  - Сети электросвязи, используемые для организации взаимодействия объектов КИИ.
- **Субъекты КИИ:**
  - Государственные органы и учреждения.
  - Российские юридические лица и индивидуальные предприниматели.
  - Организации, работающие в стратегически важных сферах (здравоохранение, транспорт, связь и др.).

2 Категоризация и значимость КИИ

Объекты КИИ делятся на **значимые** и **незначимые**. Значимые объекты КИИ (ЗОКИИ) классифицируются по категориям значимости от 1 до 3:

1. **Категория 1:** Наивысшая значимость. Нарушение безопасности может привести к серьезным последствиям.
2. **Категория 2:** Средняя значимость. Нарушение безопасности может вызвать значительный ущерб.
3. **Категория 3:** Низкая значимость. Последствия ограничены и не наносят существенного ущерба.

3 Практическое применение КИИ: сектора и примеры

КИИ охватывает широкий спектр секторов экономики и государственного управления. Примеры включают:

- **Энергетика:** Системы управления электросетями.
- **Здравоохранение:** Информационные системы больниц и медицинских учреждений.
- **Транспорт:** Управление железными дорогами, аэропортами.
- **Связь:** Телекоммуникационные сети и инфраструктура.
- **Финансы:** Банковские информационные системы.
- **Оборонная промышленность:** Системы управления оборонными объектами.

4 Как понять, относитесь ли вы к КИИ?

Чтобы понять, относитесь ли вы к КИИ, задайте себе следующие вопросы:

1. Вы работаете в одной из стратегически важных отраслей (энергетика, здравоохранение, связь и т.д.)?
2. Ваши клиенты являются субъектами КИИ?
3. Вам предъявляются строгие требования по информационной безопасности?

Если ответы на большинство вопросов положительные, ваша организация, вероятно, относится к КИИ или взаимодействует с субъектами КИИ[1].

(a) Схема субъектов и объектов КИИ

(b) Схема категорий значимости объектов КИИ

(c) Место компании-разработчика ПО в обеспечении безопасности КИИ

Список литературы

[1] ElenaGalata. *КИИ. Что это за зверь и надо ли нам его бояться*. Дек. 2024. URL: https://habr.com/ru/companies/zyfra/articles/866230/ (дата обр. 23.12.2024).

[2] SecurityVision Руслан Рахметов. *КИИ - что это? Безопасность объектов критической информационной инфраструктуры*. Май 2020. URL: https://www.securityvision.ru/blog/kii-chto-eto/?ysclid=m50zyy57ya14823063 (дата обр. 23.12.2024).