Сегодня я хочу рассказать вам о том, как обеспечивается информационная безопасность на предприятии, которое применяет Промышленный Интернет вещей.

Промышленный Интернет вещей (Industrial Internet of Things, IIoT) - это технология, которая позволяет собирать и обрабатывать данные с различных устройств и оборудования, используемых в промышленности. Однако, сбор и обработка данных может привести к угрозам информационной безопасности, поэтому необходимы меры для ее обеспечения.

**Слайд 2: Введение**

На следующих слайдах я расскажу о том, какие меры обеспечивают информационную безопасность на предприятии, которое применяет IIoT (Промышленный Интернет вещей).

**Слайд 3: Аутентификация и авторизация**

Аутентификация и авторизация - это основные меры для обеспечения безопасности в сети IIoT. Аутентификация позволяет убедиться в том, что пользователь или устройство являются тем, за кого они себя выдают. Авторизация определяет, какие действия могут выполнять аутентифицированные пользователи или устройства.

**Слайд 4: Шифрование данных**

Шифрование данных - это процесс преобразования информации в непонятный для посторонних вид. Шифрование данных позволяет защитить информацию от несанкционированного доступа и использования.

**Слайд 5: Мониторинг сети**

Мониторинг сети - это процесс наблюдения за сетью и ее устройствами с целью выявления необычной активности. Мониторинг сети позволяет быстро обнаруживать и реагировать на угрозы информационной безопасности.

**Слайд 6: Защита от вредоносных программ**

Защита от вредоносных программ - это меры, направленные на предотвращение внедрения вредоносных программ в сеть и устройства. Для этого используются антивирусные программы, брандмауэры и другие средства защиты.

**Слайд 7: Физическая безопасность**

Физическая безопасность - это меры, направленные на защиту физических объектов, таких как серверные комнаты, от несанкционированного доступа. Для этого используются системы контроля доступа, видеонаблюдение и другие средства защиты.

**Слайд 8: Обучение персонала**

Обучение персонала - это важный аспект обеспечения информационной безопасности. Персонал должен знать о возможных угрозах и уметь предотвращать их. Для этого проводятся тренинги и обучающие программы.

**Слайд 9: Резервное копирование данных**

Резервное копирование данных - это процесс создания копий данных для их защиты от потери или повреждения. Резервные копии могут быть использованы для восстановления данных в случае их потери.

**Слайд 10: Мониторинг устройств**

Мониторинг устройств - это процесс наблюдения за устройствами, используемыми в сети IIoT, с целью выявления неисправностей и угроз информационной безопасности. Мониторинг устройств позволяет быстро реагировать на проблемы и предотвращать их возникновение.

**Слайд 11: Использование сетевых сегментов**

Использование сетевых сегментов - это меры, направленные на разделение сети на отдельные сегменты с целью уменьшения риска распространения угроз информационной безопасности. Каждый сегмент может иметь свои правила доступа и уровень безопасности.

**Слайд 12: Использование VPN**

Использование VPN - это меры, направленные на защиту передачи данных между устройствами в сети IIoT. VPN позволяет создать защищенный канал связи между устройствами, что уменьшает риск перехвата данных.

**Слайд 13: Использование многофакторной аутентификации**  
  
Многофакторная аутентификация — расширенная аутентификация, метод контроля доступа к чему-либо (компьютеру, сайту и так далее) в котором пользователю для получения доступа к информации необходимо предъявить более одного «доказательства механизма аутентификации».  
  
**Слайд 14: Примеры успешной реализации мер обеспечения информационной безопасности на предприятиях, которые применяют IIoT**  
  
Примеры успешной реализации мер обеспечения информационной безопасности на предприятиях, которые применяют IIoT, включают в себя использование системы контроля доступа, мониторинга сети и устройств, защиты от вредоносных программ, обучения персонала и резервного копирования данных.  
Обеспечение информационной безопасности на предприятии, которое применяет IIoT, позволяет получить ряд преимуществ, таких как повышение эффективности работы, снижение рисков и увеличение защиты данных.  
  
**Слайд 15: Какие преимущества получает предприятие и какие риски могут возникнуть?**  
  
Обеспечение информационной безопасности на предприятии, которое применяет IIoT, позволяет получить ряд преимуществ, таких как повышение эффективности работы, снижение рисков и увеличение защиты данных.

Однако, неправильная реализация мер обеспечения информационной безопасности может привести к ряду рисков, таких как утечка данных, нарушение конфиденциальности, потеря данных и нарушение работы системы.  
  
**Слайд 16: Заключение**  
В заключение, обеспечение информационной безопасности на предприятии, которое применяет IIoT, является важной задачей, которая требует применения множества мер для защиты данных и устройст