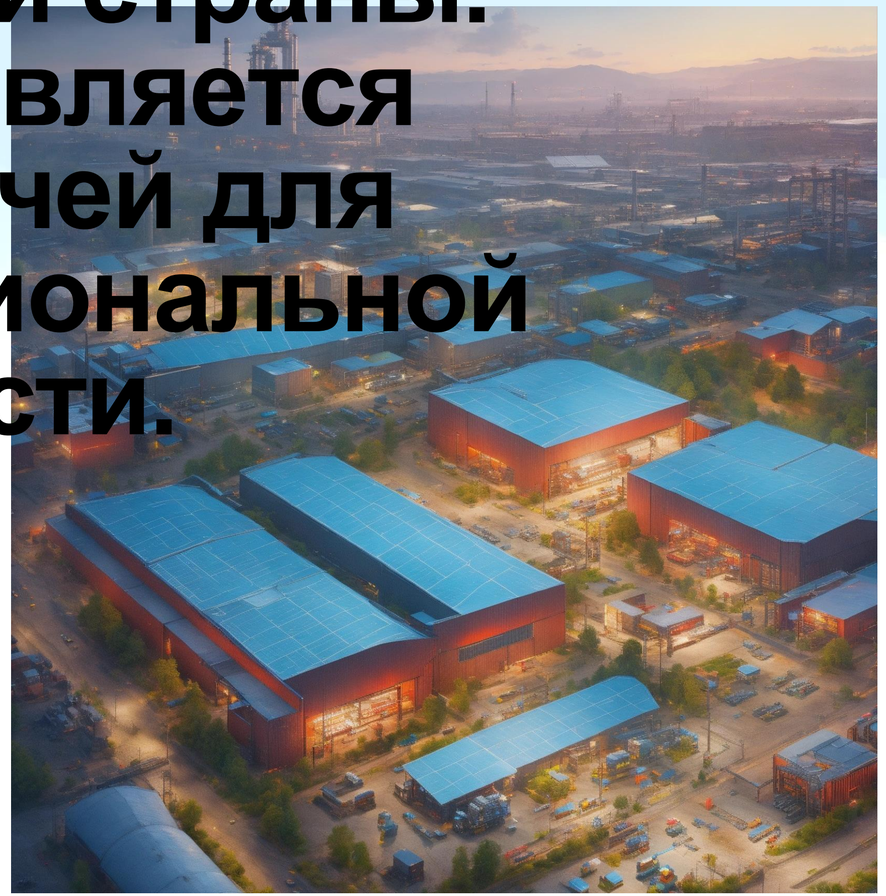
Повышения уровня защищенности ИБ

Яковенко В.И

Предприятия оборонно-промышленного комплекса ключевые элементы промышленности страны. безопасности является ключевой задачей для обеспечения национальной безопасности.

Эффективная и непрерывная работа организации отрасли — залог обороноспособности всего государства.



Текущее состояние кибербезопасности

Оборонная промышленность сталкивается с серьезными проблемами в области кибербезопасности. Хакерские атаки угрожают конфиденциальности данных и интеллектуальной собственности компаний. Необходимо усилить защиту информационных систем и сетей для предотвращения утечек данных и кражи технологий.

Ключевые цели

- Основные задачи повышения уровня киберзащищенности в оборонной промышленности включают усовершенствование систем защиты, обновление программного обеспечения и повышение осведомленности сотрудников.

Внутренние против внешних угроз

- Внутренние угрозы представляют не меньшую опасность для информационной безопасности организации, чем внешние. Сотрудники, случайно или намеренно, могут нарушить политику информационной безопасности и утечки данных. Внешние угрозы обычно исходят от хакеров, которые стремятся получить доступ к конфиденциальной информации. Однако внутренние угрозы часто труднее обнаружить и предотвратить, поскольку злоумышленники уже имеют доступ к системам и сети. Поэтому организации должны уделять одинаковое внимание защите от обеих категорий угроз.

Создание культуры безопасности

Для формирования культуры информационной безопасности в организации необходимо создать понимание важности защиты данных среди сотрудников. Это достигается путем регулярных тренингов по кибербезопасности, в которых объясняются основные угрозы и рекомендации по защите информации. Также важно поощрять бдительность персонала и давать обратную связь о правильных и неправильных действиях в области безопасности

Влияние неправильной защиты

- Несоответствие уровня информационной безопасности требованиям оборонной промышленности может привести к серьезным последствиям. Утечка секретных данных может нанести ущерб национальной безопасности и поставить под угрозу жизненно важные военные программы. Необходимо усилить меры защиты информационных систем и сетей оборонных предприятий путем внедрения последних достижений в области кибербезопасности. Это позволит обезопасить чувствительные данные и обеспечить надежность критически важной инфраструктуры.

-

Формирования культуры

Формирования культуры информационной безопасности в организации необходимо создать понимание важности защиты данных среди сотрудников. Это достигается путем регулярных тренингов по кибербезопасности, в которых объясняются основные угрозы и рекомендации по защите информации. Также важно поощрять бдительность персонала и давать обратную связь о правильных и неправильных действиях в области безопасности.

Постоянное совершенствование и адаптация Организациям необходимо регулярно оц

- Организациям необходимо регулярно оценивать и совершенствовать свои системы информационной безопасности в ответ на меняющиеся угрозы. Новые технологии и тактики хакеров требуют постоянной настройки защиты.
- Чтобы обеспечить максимальную эффективность, система информационной безопасности должна быть гибкой и адаптируемой. Необходим регулярный анализ угроз и оценка уязвимостей для своевременного внедрения усовершенствований.

Мера безопасности ОПК

Январь 2022

Введены новые правила доступа к информационным системам предприятий ОПК.

Июнь 2021

Создан Центр цифровой безопасности для координации работы по защите информации.

Декабрь 2020

Запущен пилотный проект по внедрению системы мониторинга угроз безопасности.

Июль 2019

Проведен анализ уязвимостей информационных систем и разработан план устранения.

23 млн. рублей

средний ущерб от одной атаки

45%

увеличение количества кибератак

Лучшие практики кибербезопасности

Для повышения защиты информационных систем в ОПК рекомендуется использовать комплексный подход. Следует использовать защиту на всех уровнях - от оборудования до приложений и сетевых протоколов. Регулярные проверки и тестирование позволят своевременно выявлять уязвимости до их использования злоумышленниками.

постоянный мониторинг и совершенствование политик безопасности является ключом к успешной защите данных организации.

Яковенко Владимир Игоревич
Начальник ИБ и СЗС
АО «ВТМЗ»
+79058030006
me@vyakovenko.ru