ПРОФИЛЬНЫЕ ДИСЦИПЛИНЫ:

- Защита объектов критической информационной инфраструктуры;
- Технологии искусственного интеллекта в информационной безопасности;
- Аудит информационной безопасности;
- Управление информационной безопасностью;
- Организационно-правовые механизмы обеспечения информационной безопасности;
- Защита конфиденциальной информации предприятия;
- Системы менеджмента информационной безопасности.

ОСНОВНЫЕ ИНДУСТРИАЛЬНЫЕ ПАРТНЕРЫ

КОНТАКТЫ:

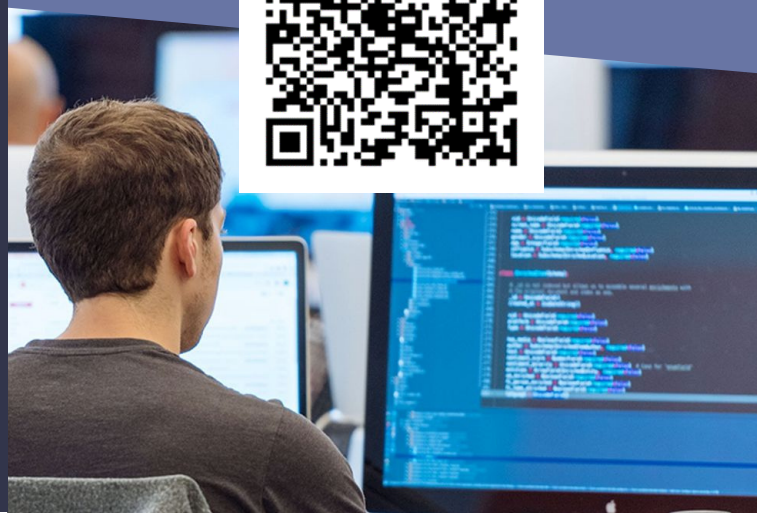
Чумилин Александр Владимирович
Телефон: +7 (3952) 40-57-44
E-mail: chumilinav@istu.edu
Аудитория: Ж-305а

ИНСТИТУТ ИТиАД

ЦЕНТР КОМПЕТЕНЦИЙ

ПО КИБЕРБЕЗОПАСНОСТИ

Направление:
10.04.01 «Информационная безопасность»
Ступень:
Магистратура
Профиль:
Безопасность киберфизических систем



АКТУАЛЬНОСТЬ НОВОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Безопасность киберфизических систем

Это обеспечение безопасности информационно-коммуникационных технологий и систем, в рамках которых изучают процессы функционирования киберобъектов, с целью выявления источников киберопасности.

Перевод большинства информационных архивов, денежных средств и коммуникаций в электронную форму создал тип актива информацию. Она подвергается посягательствам со стороны различных мошенников.

Также существенные риски возникают и в области обеспечения государственной безопасности в сфере информации.

ПРОФИЛЬНЫЕ ДИСЦИПЛИНЫ

- Теоретические и практические аспекты безопасности сетей
- Анализ угроз безопасности информации кибернетических и киберфизических систем
- Тенденции развития и появления уязвимостей в новых информационных технологиях
- Разработка новых или обновлённых сценариев безопасности для средств защиты

УЧЕБНЫЙ ПЛАН

ПРЕИМУЩЕСТВА ВЫПУСКНИКОВ И МЕСТА ТРУДОУСТРОЙСТВА

Учебная программа ориентирована на решение реальных задач:

- Проведение аудита информационной безопасности
- Проведение обследования бизнес-процессов компании, входящих в область действия СУИБ
- Разработка ИБ-стратегии с учетом выявленных рисков ИБ, проработка технических решений
- Консультирование по вопросам информационной безопасности киберфизических систем
- Разработка документированных действий СУИБ и Политики ИБ в бизнес-процессах
- Проведение оценки рисков ИБ в компании в соответствии с положениями стандарта **ISO/IEC 27005:2011**