МЫСЛИТЬ БУДУЩИМ

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Современное состояние и перспективные направления исследований в области информационной безопасности

Зегжда Дмитрий Петрович
член-корреспондент РАН, профессор РАН,
член-корреспондент Академии криптографии, д.т.н.,
директор Института компьютерных наук и кибербезопасности

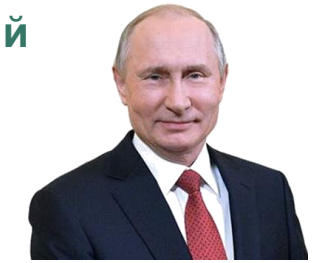
2

Союзное государство: партнеры в области кибербезопасности

ПОЛИТЕХ

“Вопрос с кибербезопасностью является одним из самых важных на сегодняшний день, потому что отключения целых систем ведут к очень тяжелым последствиям…

В.В. Путин, президент РФ



“Необходимо усиливать меры по укреплению защищенности национальной цифровой критической инфраструктуры из-за увеличения числа кибератак

М.В. Мишустин, премьер-министр РФ

“Жизнедеятельность любого государства становится все более уязвимой от компьютерных инцидентов

А.Г. Лукашенко, президент Республики Беларусь

СОЮЗНОЕ ГОСУДАРСТВО

Кибербезопасность – глобальная задача, требующая гармонизации подходов и стандартов на уровне Союзного государства

Для обеспечения кибербезопасности огромное значение имеет развитие науки и подготовка высококвалифицированных кадров

Единое киберпространство а требует согласованных действий Союзного государств по обеспечению информационной безопасности

Санкт-Петербургский Политехнический университет Петра Великого

В 2024 ГОДУ СПБПУ ОТМЕЧАЕТ 125-ЛЕТИЕ

> Наша задача сегодня — четко определить роль и значение Славянских университетов. Я твердо убежден, что мы должны смотреть на такое объединение не в парадигме двусторонних партнерских связей, а в парадигме единого пространства, единого организма, в котором идет постоянный обмен лучшими идеями, новациями и методиками.

А.И. Рудской, ректор СПбПУ

1899 ГОД ОСНОВАНИЯ

 # 3 В РЕЙТИНГЕ ВУЗОВ РФ

35 000 ВЫПУСКНИКОВ ЕЖЕГОДНО

25 АКАДЕМИКОВ И ЧЛЕН-КОРРЕСПОНДЕНТОВ

130 НАУЧНО-ИНЖЕНЕРНЫХ ЛАБОРАТОРИЙ

Лидер в подготовке профессиональных кадров по информационной безопасности

НАУЧНЫЕ ПАРТНЕРЫ СПБПУ В БЕЛАРУСИ – ВЕДУЩИЕ УНИВЕРСИТЕТЫ РЕСПУБЛИКИ

- Белорусский государственный университет информатики и радиоэлектроники
- Белорусский национальный технический университет
- Белорусский государственный университет
- Белорусско-Российский университет
- Государственное научное учреждение «Институт математики Национальной академии наук Беларуси»
- Гомельский государственный технический университет имени П.О. Сухого
- Учреждение образования "Белорусский торгово-экономический университет потребительской кооперации"
- Национальная академия наук Беларуси
- Гродненский государственный университет имени Янки Купалы
- Белорусский государственный экономический университет
- Минский государственный лингвистический университет
- Белорусский государственный технологический университет
- Институт энергетики Национальной академии наук Беларуси
- РУП «Издательство «Адукацыя і выхаванне»

БНТУ — 1920 — БЕЛОРУССКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

БГУ

БЕЛОРУССКО-РОССИЙСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ

BELARUSIAN STATE UNIVERSITY OF INFORMATICS AND RADIOELECTRONICS · 1964 ·

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

4

Институт компьютерных наук и кибербезопасности СПбПУ Петра Великого

ПОЛИТЕХ

Российская Академия Наук

Совместные научно-исследовательские работы с ИСП РАН, ИПУ РАН, ФИЦ ИУ РАН

Все уровни вузовского образования:
- Бакалавриат
- Специалитет
- Магистратура
- Аспирантура

Академия криптографии Российской Федерации

Зегжда Дмитрий Петрович является член-корреспондентом Академии криптографии, под его руководством ведутся совместные научно-исследовательские работы

Полный спектр программ подготовки по основным IT-направлениям: 02.0X.XX, 09.0X.XX, 10.0X.XX, 27.0X.XX

Все формы высшего образования:
- Очное
- Вечернее
- Заочное

5 ВЫСШИХ ШКОЛ:
- **КИБЕРБЕЗОПАСНОСТИ**
- ПРОГРАММНОЙ ИНЖЕНЕРИИ
- КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ИНФОРМАЦИОННЫХ СИСТЕМ
- УПРАВЛЕНИЯ КИБЕРФИЗИЧЕСКИМИ СИСТЕМАМИ
- ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Директор института – доктор технических наук, профессор, член-корреспондент Российской академии наук
Зегжда Дмитрий Петрович

Является действительным членом Научного совета РАН «Информационная безопасность»

4522 студентов на всех курсах!

Прием на 1 курс – более 1500 студентов!

205 преподавателей | **3 чл.-корр. РАН** | **30 профессоров** | **53 кандидата наук**

Средний возраст преподавателей института - 39 лет

5

Практико-ориентированные технологии в образовании – подготовка высококвалифицированных специалистов по информационной и кибербезопасности совместно с ведущими предприятиями и организациями Санкт-Петербурга

10.04.01_03 «Кибербезопасность нефтегазовой отрасли»

Программа обучения сформирована на основе фактических потребностей Газпром нефть в условиях активного процесса цифровой трансформации компании. В формировании учебной программы принимали участие ведущие специалисты ИБ ГПН, исходя из ежедневных задач и вызовов встающих перед ГПН.

Специализированные дисциплины для отрасли НГД:

- Киберустойчивые АСУ ТП НГД
- Безопасность VR / AR
- Безопасность КИИ
- Защищенный IioT в НГД
- Безопасная разработка ПО нефтегазовой отрасли

10.04.01_05 «Киберпсихология и безопасность Интернет-коммуникаций»

Программа «Киберпсихология» позволяет осуществлять подготовку высококвалифицированных специалистов в области кибербезопасности, обладающих не только инженерными навыками, но и аналитическими способностями на стыке различных гуманитарных наук от филологии до психологии.

- Контент как инструмент психологического воздействия и управления в информационном обществе
- Социальные сети как пространство распространения контента влияния
- Основы информационно-психологического воздействия и управления социумом
- Информационно-психологические метрики контента и Интернет-ресурсов

10.04.01_06 «Кибербезопасность беспилотных систем»

Программа направлена на подготовку магистров, обладающих опережающими компетенциями в области обеспечения кибербезопасности и киберустойчивости беспилотных систем и технологий. Магистерская программа открыта в сотрудничестве с ООО «Геоскан» и ООО «СТЦ», и носит производственно-технологический и практико-ориентированный характер.

- Технологии беспилотных устройств и самоорганизующихся сетей
- Безопасность мобильных сетей
- Методы и средства защиты беспилотных устройств и самоорганизующихся сетей
- Методы и средства противодействия целенаправленным атакам
- Основы кибербезопасности беспилотных устройств

6

NeoQUEST: игровые технологии обучения кибербезопасности с участием в командных и индивидуальных соревнованиях с использованием кибер-полигонов

ПОЛИТЕХ

Моделирование информационной инфраструктуры реальных объектов

Моделирование угроз и уязвимостей

Иммерсивное обучение за счет погружения в смоделированную уязвимую среду

Оффлайн этап – **20 сентября!**

10 лет проводится NeoQUEST

50 000 участников из России, Беларуси, Армении

NeoQUEST проводится в Санкт-Петербурге, в его программе:

- Доклады на самые актуальные вопросы практического обеспечения ИБ
- Иммерсивные воркшопы и мастер-классы по хакингу и защите
- Real-time моделирование кибератак

7

Многофункциональный учебно-научный центр по проблемам информационной безопасности в СЗФО на базе Института компьютерных наук и кибербезопасности СПбПУ Петра Великого

СПбПУ ПЕТРА ВЕЛИКОГО – база СЗРО УМО – объединение 20 вузов Северо-Западного Федерального Округа, готовящих специалистов по группе специальностей и направлений «Информационная безопасность»

Главный радиочастотный центр

Ростелеком Солар

РОСКОМНАДЗОР

ГАЗПРОМ НЕФТЬ

Многофункциональный учебно-научный центр по проблемам информационной безопасности в СЗФО на базе СПбПУ обеспечивает:

- Удаленное предоставление практико-ориентированных образовательных сервисов и средств образовательным организациям Северо-Западного федерального округа РФ
- Реализация игрового практико-ориентированного подхода к обучению за счет открытых виртуальных лабораторий
- Предоставление обучающимся доступа к виртуальным лабораториям, моделирующим информационную инфраструктуру реальных объектов (промышленных, финансовых, транспортных и т.д.)
- Предоставление широкого набора образовательных сервисов и интеллектуальных средств тестирования для преподавателей

> **С учетом опыта работы по целевой подготовке специалистов в области ИБ СПбПУ и обеспечению потребностей подразделений по защите информации в федеральном округе квалифицированными кадрами, проводимой в рамках решений Межведомственного совета по защите информации в СЗФО, поддерживаю данный проект и желаю Вам успехов в его реализации.**

А. Гуцан, полномочный представитель Президента РФ в СЗФО

Кибербезопасность как национальный приоритет

Стратегия научно-технологического развития страны до 2035 года

ПРИОРИТЕТ СТРАТЕГИИ (ПУНКТ 20Д):
Противодействие техногенным, биогенным, социокультурным угрозам, терроризму и идеологическому экстремизму, а также киберугрозам и иным источникам опасности для общества, экономики и государства

- **Указ Президента Российской Федерации № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»**
- **Указ Президента Российской Федерации № 250 «О дополнительных мерах по обеспечению информационной безопасности в Российской Федерации»**

Нацпроекты РФ «Цифровая экономика» и «Экономика данных»

НАПРАВЛЕНИЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
Обеспечение безопасности цифрового пространства, защита персональных данных граждан, защита от киберугроз

“Киберпреступность переходит из реального сектора в виртуальный, и без целостного противодействия кибермошеничеству невозможно обеспечить надежность и доверие цифровым сервисам

Шойтов А.М., зам. министра Минцифры РФ

Перспективные задачи кибербезопасности, актуальные для Союзного государства

ПРОМЫШЛЕННОСТЬ

Обеспечение киберустойчивости промышленной инфраструктуры

ОБЩЕСТВО

- Защита общества от когнитивного воздействия в медиапространстве
- Защита персональных данных от неправомерных действий с ними

ЭКОНОМИКА

Защита цифровых финансовых активов от специфичных киберугроз

АРМИЯ

Обеспечение кибербезопасности задач и операций, выполняемых беспилотными летательными аппаратами

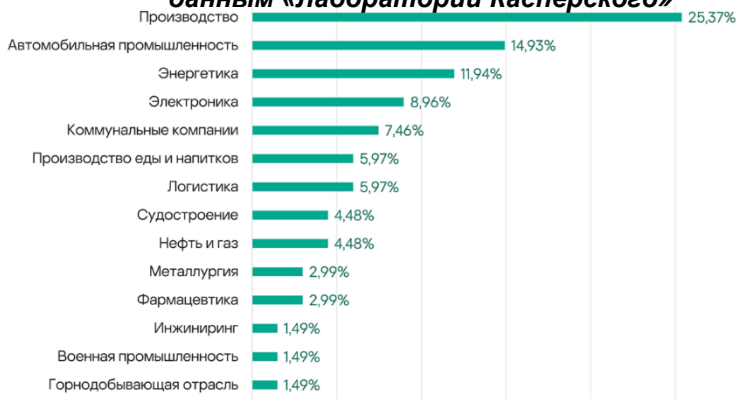
ТЕХНОЛОГИИ

- Защита от киберугроз, порождаемых искусственным интеллектом
- Создание защищенной инфраструктуры передачи данных с применением квантовых вычислений

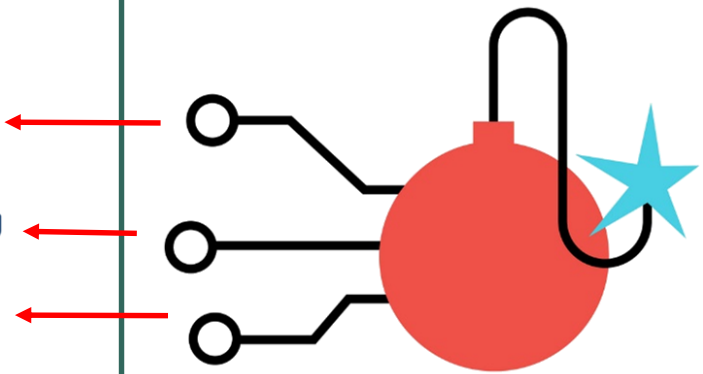
Кибератаки на промышленную инфраструктуру – глобальная угроза

КИБЕРФИЗИЧЕСКИЕ СИСТЕМЫ

Статистика атак на промышленность по данным «Лаборатории Касперского»



ПРОМЫШЛЕННЫЕ ОБЪЕКТЫ РАЗЛИЧНЫХ ОТРАСЛЕЙ РЕГУЛЯРНО ПОДВЕРГАЮТСЯ КИБЕРАТАКАМ



КИБЕРАТАКИ

- Вывод из строя промышленных объектов инфраструктуры
- Перехват управления промышленными системами
- Внутреннее воздействие на систему с целью спровоцировать технологическую катастрофу

Обеспечение киберустойчивости промышленной инфраструктуры

4 600 000
КИБЕРАТАК
отразила Московская система электронного голосования за время выборов президента РФ с 15 по 17 марта 2024 г.

200 000
КИБЕРУГРОЗ
фиксируется в РФ каждую минуту

Учитывая высокую интенсивность и непрекращающийся рост числа кибератак, необходимо обеспечивать корректное функционирование промышленных объектов даже в условиях деструктивных информационных воздействий

КИБЕРУСТОЙЧИВОСТЬ

Способность системы выполнять свои функции в условиях успешно реализованных кибератак на ее ресурсы (возможно, несколько менее эффективно в течение периода времени, необходимого для нейтрализации кибератак и устранения их последствий)

Перспективные направления исследований

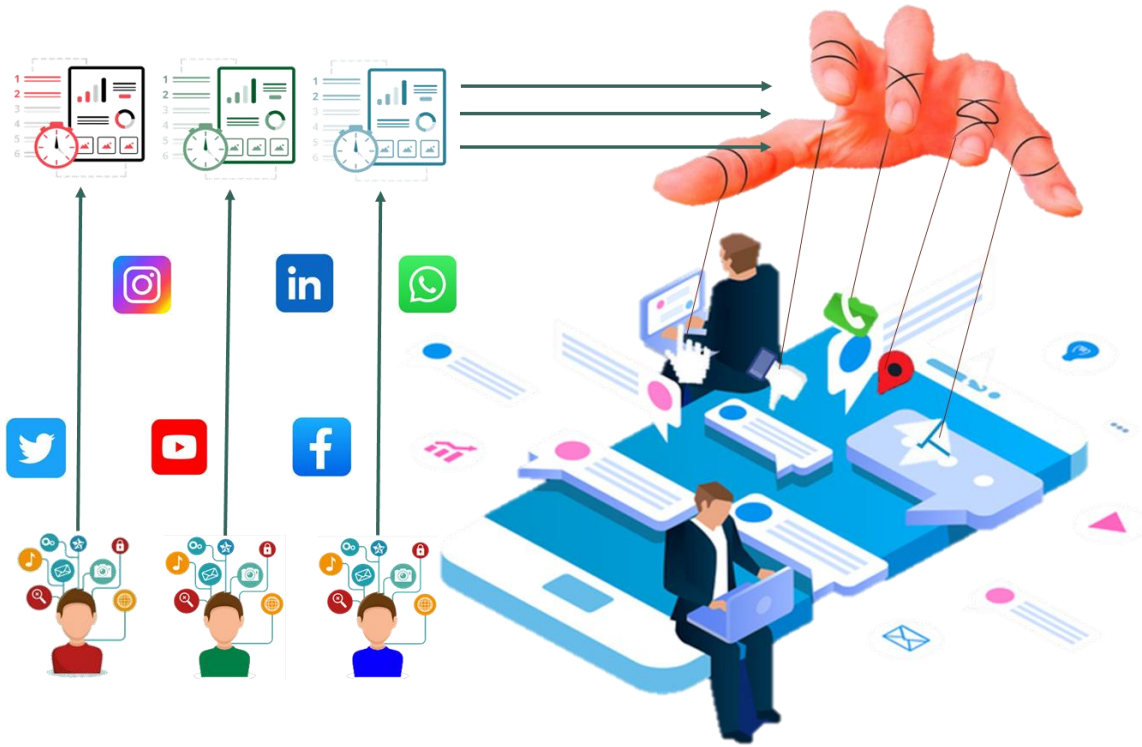
- **Моделирование промышленной инфраструктуры с использованием иммерсивных кибер-полигонов, для отработки сценариев реагирования на инциденты**
- **Создание методологии построения кибер-иммунных систем для обеспечения функционирования промышленных объектов в условиях атак**
- **Разработка технологии анализа больших объемов данных для обеспечения киберустойчивости при массированных и мощных кибератаках**

Когнитивные воздействия на общество в медиапространстве

5 350 000 000
УЧАСТНИКОВ МЕДИАПРОСТРАНСТВА В МИРЕ*

127 600 000
УЧАСТНИКОВ МЕДИАПРОСТРАНСТВА В РОССИИ

+ 266 000 000
НОВЫХ УЧАСТНИКОВ МЕДИАПРОСТРАНСТВА ЗА 2023 ГОД



~300 МИНУТ В ДЕНЬ МОЛОДЕЖЬ ПРОВОДИТ В МЕДИАПРОСТРАНСТВЕ

- **Медиапространство стало неотъемлемой частью жизни общества за счет переноса коммуникаций в Интернет**
- **Для автоматического формирования таргетированного контента и распространения дезинформации в медиапространстве используется искусственный интеллект**
- **Когнитивное воздействие в медиапространстве – мощный инструмент целенаправленного влияния на массовое сознание общества**

**По данным компании масс-медиа We Are Social*

Защита общества от когнитивных воздействий в медиапространстве

Перспективные направления научных и прикладных исследований

Формирование научно-методологической базы для определения контента, созданного искусственно путем применения методов машинного обучения

Выявление информационных кампаний на основе интеллектуальной технологии структурно-семантического анализа данных медиапространства

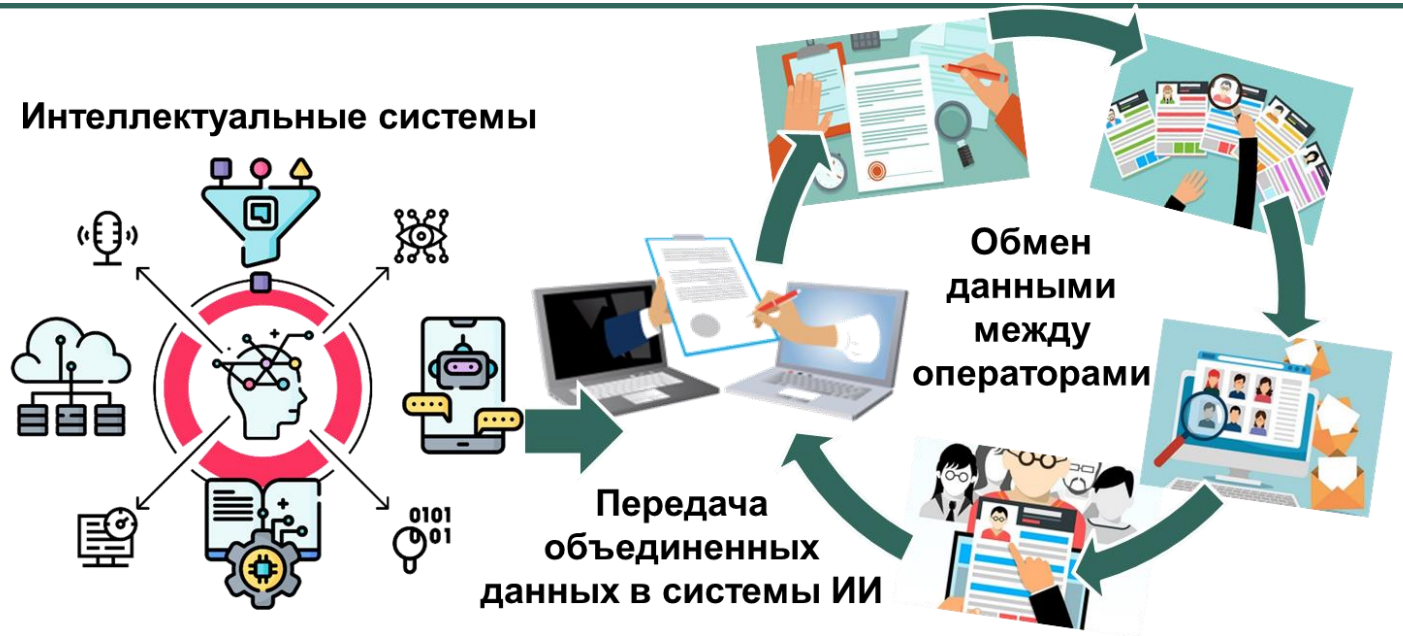
Проведение киберпсихологических исследований по способам формирования специализированного контента, обеспечивающего продвижение идеологии государства в медиапространстве

Противодействие утечкам персональных данных (ПДн) о гражданах

Использование ПДн в системах ИИ

биометрические системы | **медицинские сервисы** | **системы страхования и кредитования**

- Системам искусственного интеллекта требуются большие объемы данных из разных источников для обучения и работы
- При объединении данных или при атаках на систему ИИ могут произойти утечки ПДн



Перспективные направления научных и прикладных исследований

- **Использование методов защищенной обработки ПДн без доступа к их содержимому с применением механизмов гомоморфного шифрования**
- **Обучение моделей искусственного интеллекта без обмена данными между источниками с помощью федеративного обучения**

Защита цифровых финансовых активов (ЦФА) от киберугроз

ЦФА – новых цифровые финансовые активы и цифровые валюты, учет и обращение которых возможен только путем внесения записей в распределенный реестр (блокчейн)

Майнинг –деятельность по созданию, перераспределению, использованию ЦФА и цифровых валют

Виды майнинга основаны на преобразовании следующих видов экономических ресурсов:

энергетические ресурсы

время, затрачиваемое людьми

права собственности на уникальные объекты (как реальные, так и виртуальные)

Новые угрозы экономической и информационной безопасности

- дестабилизация и обесценивание национальной экономики за счет целенаправленного провоцирования затрат реальных экономических ресурсов
- мгновенное изъятие/уничтожение ценностей и возможность введения односторонних санкций для отдельных участников

Перспективные направления исследований

- Разработка криптографических механизмов для защиты от неправомерной аутентификации третьих лиц на платформе обращения ЦФА с использованием технологии распределенного реестра
- Предотвращение потери ЦФА отечественных компаний на основе интеллектуального поведенческого анализа участников и пользователей платформы обращения

Обеспечение кибербезопасности задач и операций, выполняемых беспилотными летательными аппаратами (БПЛА)

ПОЛИТЕХ

ПРОГРАММНЫЕ ХАРАКТЕРИСТИКИ

АЭРОДИНАМИЧЕСКИЕ ХАРАКТЕРИСТИКИ

ЭНЕРГЕТИЧЕСКИЕ ХАРАКТЕРИСТИКИ

ФИЗИЧЕСКИЕ ХАРАКТЕРИСТИКИ

УРОВЕНЬ ПРОГРАММНЫХ ХАРАКТЕРИСТИК БПЛА

- защита от кибератак
- возможности для кибервоздействия на БПЛА противника

ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ ИССЛЕДОВАНИЙ С УЧЕТОМ СВО

Обеспечение защищенного помехоустойчивого гео-позиционирования

Оценка доверенности для отечественной компонентной базы, используемой в БПЛА

Разработка малоресурсных криптографических механизмов для БПЛА с целью защиты канала связи

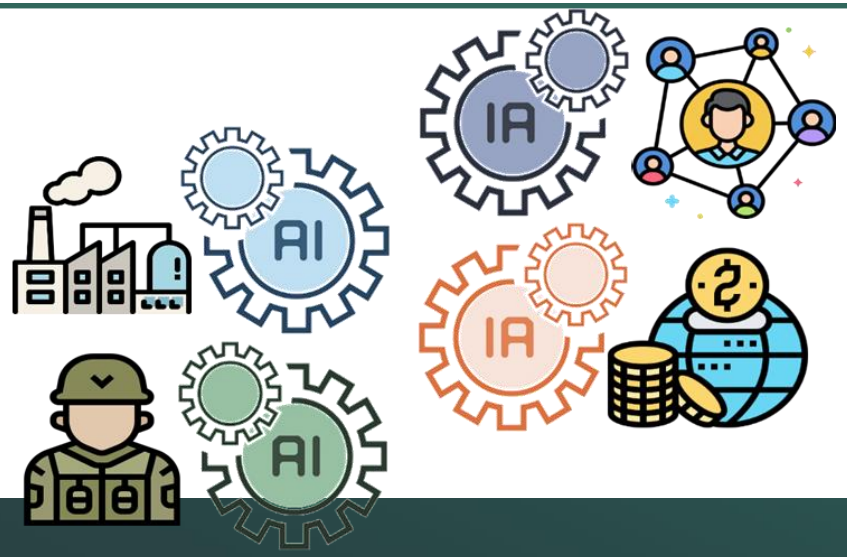
Создание методов и техник выявления уязвимых мест в программном обеспечении вражеских БПЛА и кибервоздействия на них

Искусственный интеллект (ИИ) и кибербезопасность

Искусственный интеллект – это аппроксимация функции отображения некоторого множества бесконечной размерности в заданное конечномерное множество

Проблема построения аппроксимации функции отображения бесконечномерного пространства в конечномерное относится к категории некорректных задач, решение которых либо отсутствует, либо множественно, либо неустойчиво

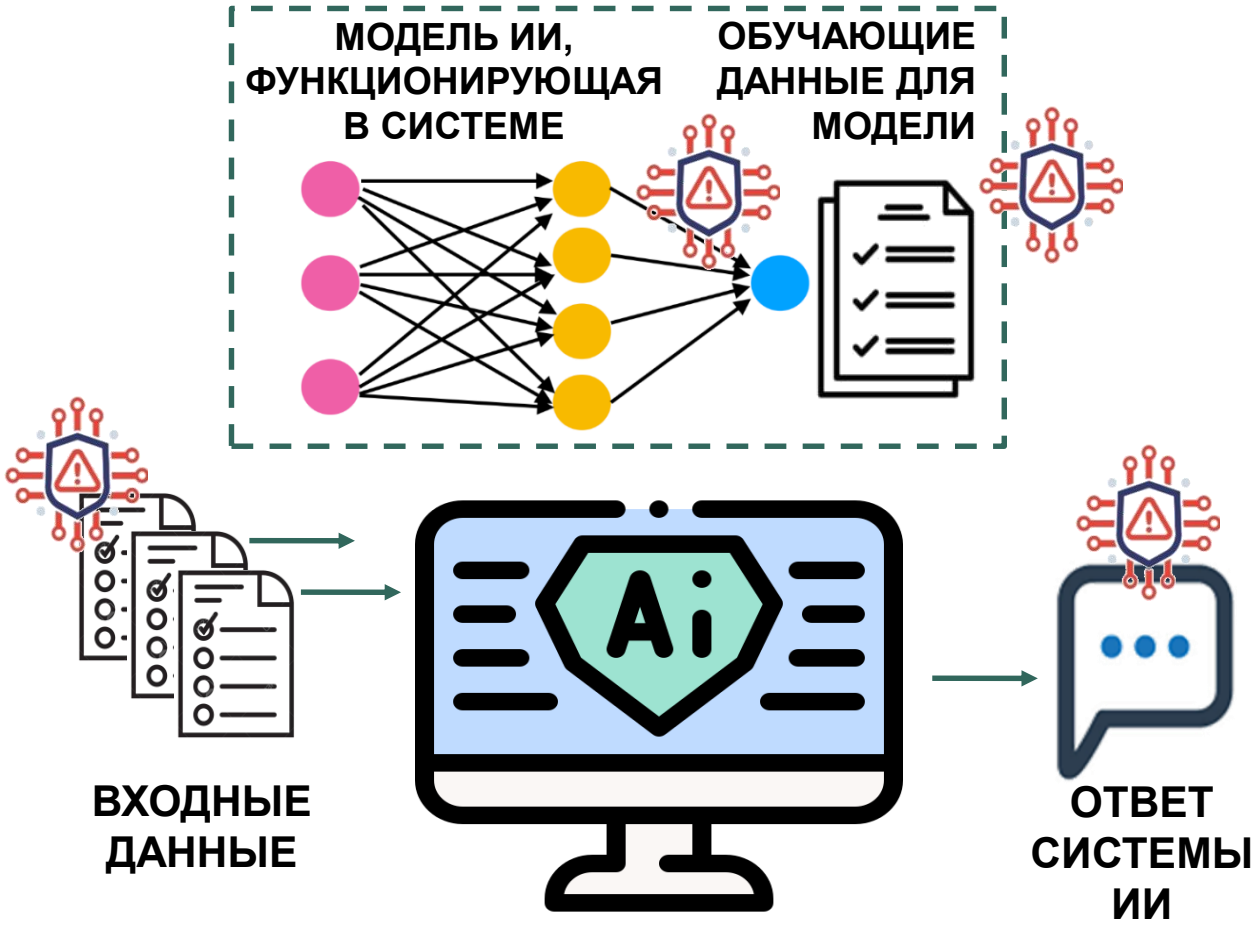
Технологии ИИ используются во всех сферах деятельности: промышленность, общество, экономика, армия



НОВЫЕ КИБЕРУГРОЗЫ, ПОРОЖДАЕМЫЕ ИИ

- **Намеренное формирование нерепрезентативных обучающих наборов данных**
- **Иллюзия пользователей и разработчиков интеллектуальных систем о непогрешимости ИИ**
- **Воздействия на модели ИИ, вследствие которых системы ИИ принимают некорректные решения**
- **Утечка ПДн пользователей систем ИИ**
- **Утечка сведений о принципах реализации системы ИИ**

Защита систем ИИ от киберугроз



- **ЗАЩИТА ОБУЧАЮЩИХ ДАННЫХ ОТ КИБЕРУГРОЗ**
  - АНАЛИЗ СЛУЧАЙНОСТИ И РЕПРЕЗЕНТАТИВНОСТИ ОБУЧАЮЩИХ ДАННЫХ
  - ЗАЩИТА ОБУЧАЮЩИХ ДАННЫХ ОТ МОДИФИКАЦИИ
  - ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ОТ УТЕЧЕК
- **ЗАЩИТА МОДЕЛИ ИИ ОТ КИБЕРУГРОЗ**
  - ЗАЩИТА ИНФОРМАЦИИ О ПАРАМЕТРАХ ОБУЧЕНИЯ МОДЕЛИ
  - ИСКЛЮЧЕНИЕ ВОЗМОЖНОСТИ НЕСАНКЦИОНИРОВАННОГО ВЛИЯНИЯ НА ПРОЦЕСС ОБУЧЕНИЯ
- **ЗАЩИТА СИСТЕМЫ ИИ ОТ КИБЕРУГРОЗ**
  - ВЫЯВЛЕНИЕ ВОЗМОЖНЫХ ПРОГРАММНЫХ ЗАКЛАДОК
  - ПРОВЕРКА УСЛОВИЙ РЕГИСТРАЦИИ ВХОДНЫХ ДАННЫХ
  - ЗАЩИТА ВХОДНЫХ ДАННЫХ ОТ МОДИФИКАЦИИ

Перспективные направления научных и практических исследований

Разработка методологии выявления и нейтрализации программных закладок в моделях ИИ на основе идентификации их триггеров для противодействия атакам на целевую систему

Создание технологии безопасной агрегации обучающих наборов данных использованием гомоморфного шифрования для обучения отечественных крупномасштабных интеллектуальных систем

Разработка комплекса методов и алгоритмов обратного восстановления параметров моделей ИИ для определения принципов построения зарубежных систем ИИ и их воссоздания

Технологии квантовых вычислений для решения задач экономики данных и оборонно-промышленного комплекса

Квантовые вычисления

Объединяют аспекты информатики, физики и математики, используют квантовую механику для ускорения решения сложных проблем по сравнению с классическими компьютерами

- Ускоряют решение задач, специально сформулированных для этого типа вычислительных устройств
- Радикально ускоряют решение трансвычислительных задач комбинаторного характера

Зарождение квантовой информатики

Квантовые вычислители могут расширить возможности по решению задач, которые уже сформулированы для традиционных компьютеров, но решаются недостаточно эффективно из-за большой размерности или требуемой высокой точности.

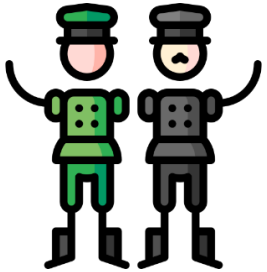
Перспективные направления исследований

- Разработка гибридных алгоритмов квантовых вычислений для различных задач экономики данных и оборонно-промышленного комплекса
- Исследование подходов и технологий создания универсальной программной платформы квантовых вычислений
- Формирование методологии оценки защищенности квантовых систем от киберугроз

Задачи в области информационной безопасности для совместного решения Союзным государством

Гармонизация учебных программ для согласованной подготовки высококвалифицированных кадров

Объединение усилий ведущих научных центров для скоординированного проведения научно-технических исследований в области кибербезопасности



Международное сотрудничество в борьбе с киберпреступностью и кибертерроризмом с учетом опыта СВО

1 2 5

ПОЛИТЕХ

Мы уверенно смотрим вперед, планируем свое будущее, намечаем и уже реализуем новые проекты и программы, которые призваны сделать наше развитие еще более динамичным, еще более мощным.

Мы единый и великий народ и вместе преодолеем все преграды, воплотим в жизнь все задуманное. Вместе победим!

В.В. Путин, президент РФ

23

33-я научно-техническая конференция

МЕТОДЫ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

имени Петра Дмитриевича Зегжды

125

ПОЛИТЕХ

Конференция «Методы и технические средства обеспечения безопасности информации» (МиТСОБИ) – это встреча профессионалов информационной безопасности, единственная и старейшая конференция сферы ИБ, **с 1991 года** ежегодно проходящая в Санкт-Петербурге.

Темы 33-й НТК МиТСОБИ :

- Искусственный интеллект в задачах ИБ: теория и практика;
- Социальные коммуникации цифрового общества: доверие и безопасность;
- Кибербезопасность объектов КИИ
- Криптографические методы защиты информации
- Подготовка кадров в сфере ИБ;
- Вопросы информационной безопасности в работах молодых ученых

Даты проведения: 24-27 июня 2024 года

г. Санкт-Петербург, п. Репино, ул. Луговая, д.10, лит. А, отель «ForRestMix»

Санкт-Петербургский политехнический университет Петра Великого

Контакты:

kafedra@ibks.spbstu.ru
Тел.: 552-76-32

Зегжда Дмитрий Петрович
Директор ИКНК,
чл.-корр. РАН, д.т.н., проф.