



УНИВЕРСИТЕТ ИТМО

ФБИТ

Методология подготовки специалиста по кибербезопасности

ИСТОРИЯ ФАКУЛЬТЕТА

Создан в 2017 г. из 4-х кафедр
Новая команда

СЕГОДНЯ

120

сотрудников
($\frac{1}{2}$ имеет
научную
степень)

1100

студентов

100

аспирантов

1500

выпускников



ФАКУЛЬТЕТ

Образовательные программы

Научно-образовательный центр

Фокус развития факультета

Математические методы защиты, обработки и хранения информации

Валидация сложных технических систем (в части безопасности)

Исследование стека технологий защиты информации



МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА



КЛЮЧЕВЫЕ ПАРТНЕРЫ



Фокусировка факультета — информационная и кибербезопасность, информационно-функциональная безопасность (ИФБ).



БОЛЬШОЙ ВЫЗОВ

Снижение уровня безопасности современных информационных и киберфизических систем в условиях растущего числа мобильных устройств, «умных» вещей, обменивающихся колоссальными объемами информации без должного контроля со стороны человека.

М-ПЛАТФОРМА

ИФБ – среда (методология, средства и способы) подготовки исследовательских кадров высокой квалификации и проведения научной и проектной деятельности по обеспечению ИФБ и обоснованного доверия к инновационным продуктам и сервисам.

РАЗРАБОТКА СЕРВИСОВ

SECURE
BY DESIGN

СЕРТИФИКАЦИЯ
И СОПРОВОЖДЕНИЕ



ДОВУЗОВСКАЯ ПОДГОТОВКА: ОТБИРАЕМ ЗВЕЗД

МЕРОПРИЯТИЯ

Реализация довузовских программ
Спецплощадка в Аничковом лицее
Школьные группы спец.подготовки на базе ФБИТ (43 человека)
Олимпиада «Математика и криптография им. Верченко»
Олимпиада ITMO Security
Рабочая база из 63 математических школ России
Движение CTF Kids

РЕЗУЛЬТАТЫ:

Набор мотивированных ребят, которые знают ФБИТ
ЕГЭ 280 баллов
“Поступай не как все”
50% контрактники



ОБРАЗОВАТЕЛЬНЫЕ ПРОГРАММЫ

Сетевые взаимодействия

Коллектив > 50% сотрудников работают в индустрии

Уникальная цифровая образовательная платформа
по кибербезопасности

МАГИСТРАТУРА

- Кибербезопасность в банковской сфере
 - Криптографические методы защиты информации
 - Информационная безопасность специализированных систем
 - Информационная безопасность компьютерных систем
- Функциональная безопасность критически важных систем



ВНЕУЧЕБНАЯ ДЕЯТЕЛЬНОСТЬ

Управление внеучебным временем

Национальный Полигон "Ростелеком"

Учебно-практический центр "Киберполигон"

Этичный хакинг



РЕГУЛЯРНЫЕ ПОБЕДЫ НА СОРЕВНОВАНИЯХ:



СуBRICS CTF 2021 – крупнейшие международные соревнования от Российских организаторов: 500 команд из 49 стран мира

Олимпиада "Я профессионал"

CodeX Lab ведущие разработчики open-source проектов и фавориты github

CTFClub – тренируем весь Петербург

Участие в CTFClub – значимое преимущество при устройстве на работу

НАУКА

ЛАБОРАТОРИИ

- Средства Криптографической защиты информации
- Теория Информации и Кодирования
- Мультиагентные Системы
- ПО
- ИБ Киберфизических Систем

ФОКУСИРОВКА

- Технологий AI
- IoT и роботизированных систем
- Облачных технологий в контексте развития сетей 5G
- Компьютерных систем.

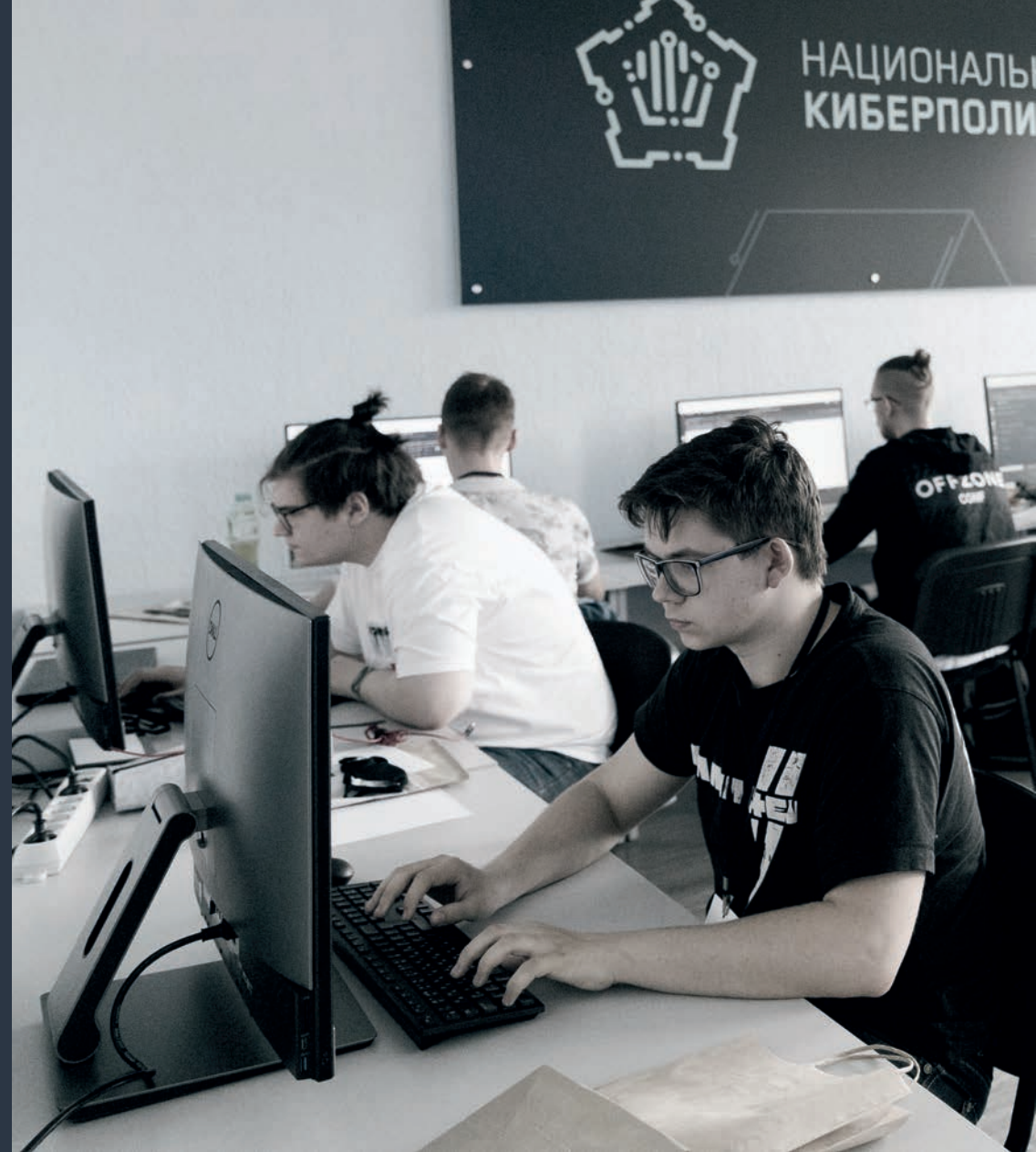
Результаты 2022

31% работ
Федерального
уровня

Реальные
внедрения

Разработки
по внешним
заказам

Гособоронзаказ



УСТОЙЧИВОСТЬ К ВЫСОКИМ ПОВТОРЯЕМЫМ РЕЗУЛЬТАТАМ



**МЫ СТРЕМИМСЯ ВЫЙТИ
ЗА ПРЕДЕЛЫ УНИВЕРСИТЕТА**





РИСКИ И РЕШЕНИЯ

С одной стороны, конкуренция с бизнесом за кадровый потенциал
С другой – индустрия воспринимает ИБ, как налог, а не как жизненную необходимость.
Ситуацию необходимо менять с помощью рассудительно-доказательной базы

Инициативное направление "Безопасность цифровых медицинских технологий"

Цель направления: развитие подходов к обеспечению информационной безопасности медицинских данных и сложных медицинских систем как отдельного вида распределённых мультиагентных и киберфизических систем

Проекты и партнеры:

Цифровой двойник пациента, методы обезличивания и анонимизации данных при обработке в медицинских системах, совершенствование процессов моделирования угроз и оценки рисков информационной безопасности для перспективных медицинских систем, методы обеспечения безопасности устройств медицинского интернета вещей

Задачи направления:

- разработка **новых цифровых технологий** в области общественного здоровья;
- оценка **эффективности и безопасности** этих технологий;
- моделирование угроз и оценка рисков информационной безопасности для перспективных медицинских систем;

Состав: 1 д.т.н., 1 д.м.н. (ВМедА), 2 к.т.н., аспиранты, магистранты и бакалавры

Университет ИТМО, г. Санкт-Петербург, <https://securityhub.ru>

Связаться с лабораторией: vmkorzhuk@itmo.ru

Лаборатория

«Цифровые технологии в общественном здоровье»

Миссия лаборатории: Трансформация системы общественного здоровья в Санкт-Петербурге путем внедрения программ скрининга и диагностики социально-значимых заболеваний с помощью новых цифровых решений, основанных на совершенствовании подходов к сбору больших медицинских данных и применении систем искусственного интеллекта

Основана в ноябре 2022

Проекты и партнеры:

Яндекс.Облако, СПИРАЛ (ФГБУ «СПб НИИФ» Минздрава России), ФГБУ «НМИЦ онкологии им. Н.Н. Петрова» Минздрава России, Скандинавия, Ильинская больница

Задачи лаборатории:

- разработка **новых цифровых технологий** в области общественного здоровья;
- **оценка эффективности этих технологий** для проведения скрининга и ранней диагностики;
- **изучение различных эффектов внедрения технологий** (в том числе социальных и экономических);
- **внедрение решений** на уровне медицинских партнеров и города.

Состав: 13 научных сотрудников (5 сотрудников из сферы ИТ, 5 сотрудников из медицины, 3 сотрудника из социальных наук), 2 инженера, 1 техник
4 стажера (3 стажера из Университета ИТМО, 1 стажер из СПбАУ им. Ж. И. Алфёрова)

Университет ИТМО, г. Санкт-Петербург, <https://dpht.itmo.ru/>

Связаться с лабораторией: dpht1014@itmo.ru

Выводы

База есть

ГОТОВЫ К МАСШТАБИРОВАНИЮ