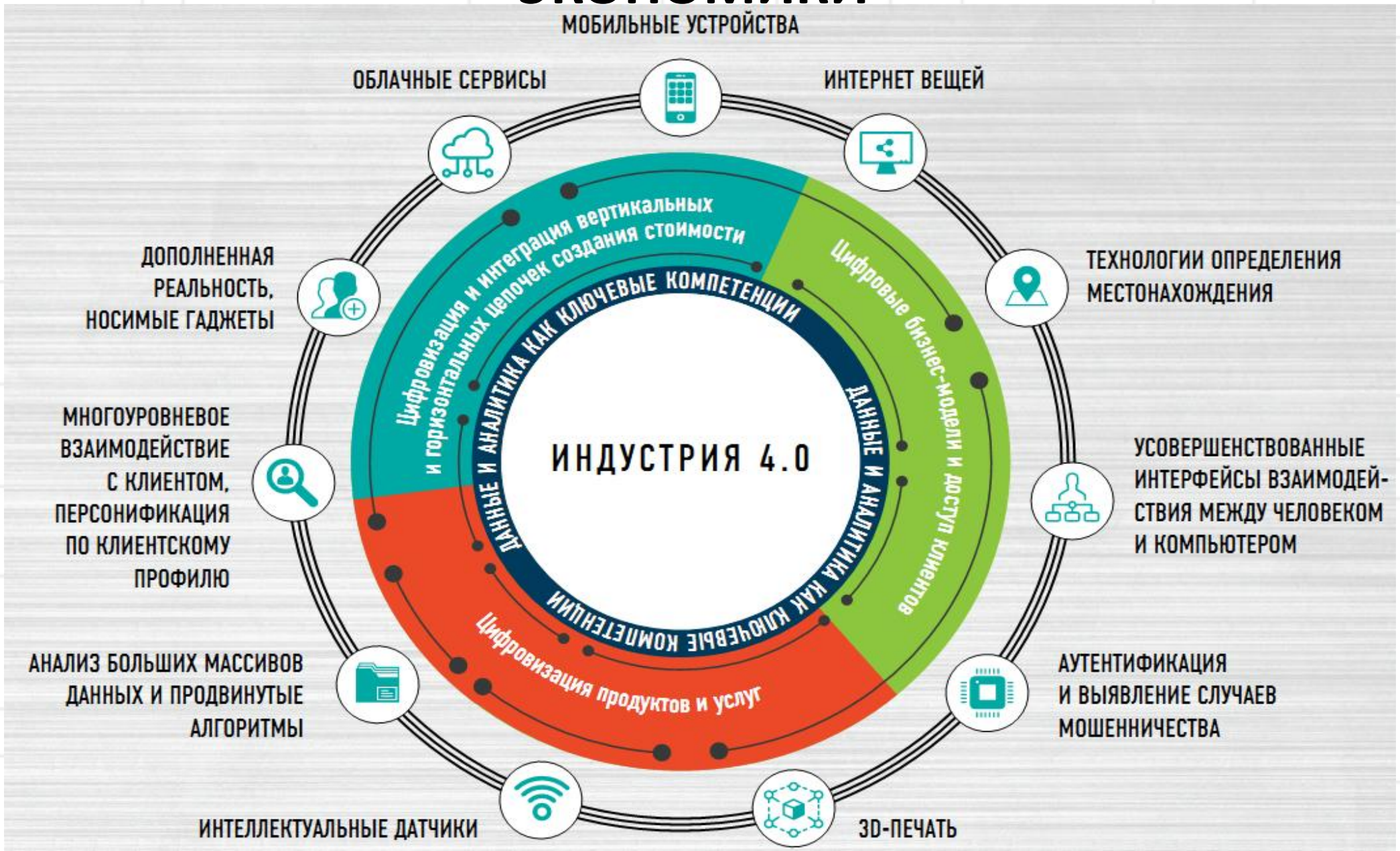
ПОЛИТЕХ
Санкт-Петербургский
политехнический университет
Петра Великого

НОВЫЕ ВЫЗОВЫ БЕЗОПАСНОСТИ И ФОРМИРОВАНИЕ КОМПЕТЕНЦИЙ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. СОЗДАНИЕ НАУЧНО-ОБРАЗОВАТЕЛЬНОГО КЛАСТЕРА.

Зегжда П.Д. - руководитель отделения «Кибербезопасность»,
д.т.н., профессор, заслуженный деятель науки РФ
ИПММ, ФГАОУ ВО «Санкт-Петербургский политехнический
университет Петра Великого»

«РусКрипто'2019»
19 - 22 марта 2019 г.

ИНТЕГРАЦИОННАЯ ЦИФРОВИЗАЦИЯ ПЛАТФОРМ ЦИФРОВОЙ ЭКОНОМИКИ



Новые вызовы - новые задачи кибербезопасности

ХАБ КИБЕРБЕЗОПАСНОСТИ
Новые агрегирующие и интеллектуальные технологии

БЕЗГРАНИЧНОСТЬ КИБЕРСРЕДЫ

- **Гигантское число** пользователей, узлов, потоков информации и управления
- **Нечеткий** периметр одноранговых инфраструктур
- **Автоматизация** администрирования **разнородных** компонентов
- Мониторинг и управление = **проблема «больших данных» и «умных решений»**

МОБИЛЬНОСТЬ КИБЕРСРЕДЫ

- **Перемещение** узлов, **высокая динамика** топологии
- **Отсутствие** фиксированной связности узлов
- **Ограничение вычислительной мощности** узлов
- **Сложность** соблюдения **единой** надсистемной и **согласованной** с ней внутрисистемной политики безопасности
- Необходимость **непрерывного** управления и контроля доступа

Новые задачи безопасности

ГЛОБАЛЬНОЕ ДОВЕРИЕ

КОГНИТИВНОСТЬ

БОЛЬШИЕ ДАННЫЕ

ДЕЦЕНТРАЛИЗАЦИЯ

АДАПТИВНОСТЬ

КИБЕРУСТОЙЧИВОСТЬ

В области подготовки специалистов по ИБ

Вызов: создание доверенного киберпространства, обеспечение киберустойчивости.

Ответ: специалист должен владеть методами решения следующих задач:

- Обнаружение и анализ киберугроз, направленных на нарушение киберустойчивости систем цифрового производства и цифровой экономики, робототехнических систем
- Реализация адаптивной активной системы предотвращения киберугроз с использованием методов искусственного интеллекта для управления параметрами и архитектурой защищенной системы
- Разработка методов безопасной обработки больших и сверхбольших массивов данных с использованием гомоморфной криптографии, создание глобальной доверенной среды с использование блокчейн и оптимизация информационных потоков на основе BigData.
- Разработка систем мониторинга, оценки состояния, расследования инцидентов кибербезопасности и киберустойчивости для прогнозного управления безопасностью цифрового пространства

Общетеоретическая подготовка специалистов должна базироваться на следующих областях знаний

- **Управление информационной безопасностью:** методы организации адаптивной динамической системы со стохастическими характеристиками, адаптивное управление с использованием искусственного интеллекта.
- **Криптографическая защита:** гомоморфная криптография, распределенные постквантовые криптоалгоритмы, криптографическая защита в децентрализованных распределенных самоорганизующихся сетях, блокчейн.
- **Безопасность больших данных:** принципы работы с большими данными, защищенные системы интеллектуального сбора и предобработки неструктурированных данных, анализ данных в облачных системах и на гетерогенном вычислительном кластере, применение гомоморфной криптографии для обработки больших и сверхбольших массивов данных, методы динамического управления нагрузкой.
- **Киберугрозы и киберустойчивость систем цифрового производства:** методы обеспечения глобального доверия и киберустойчивости, методы глубокого обучения для обнаружения уязвимостей в программном обеспечении, анализа вредоносных программ, распознавания сетевых атак, обнаружения бот-сетей и кибермошенничества.

Специалист должен владеть современными информационными технологиями

- Сетевые технологии: сети с переменной архитектурой, самоорганизующиеся сети, магистральные сети
- Гибкие сети
- Облачные и туманные системы
- Эластичные и мягкие вычисления
- Суперкомпьютерные технологии
- Технологии искусственного интеллекта
- Современные базы данных
- Интегрированные мобильные системы

Причины недостаточности компетенций специалистов по ИБ.

1. Несоответствие темпов развития ИТ и совершенствования

нормативной базы и системы стандартов по информационной безопасности.

2. Инерционность системы модификации образовательных программ.

3. Противоречия между локальностью задач производства и бизнеса и универсальностью и мобильностью образования.

4……..

ВЫВОД: Создание системы взаимодействия бизнеса и ВУЗов.

Подготовка специалистов на кафедре ИБКС ФГАОУ ВО «СПбПУ»

10.05.01 – Компьютерная безопасность (5,5 лет)

Специализации:

- **Математические методы защиты информации**
- **Безопасность программного обеспечения мобильных систем**

ЕГЭ: математика, ФИЗИКА, русский язык

41 чел.

10.05.03 – Информационная безопасность автоматизированных систем (5 лет).

Специализация: **Анализ безопасности информационных систем**

ЕГЭ: математика, ИНФОРМАТИКА, русский язык

41 чел.

10.05.04– Информационно-аналитические системы безопасности (5,5 лет)

Специализация: **Автоматизация информационно-аналитической деятельности**

ЕГЭ: математика, ИНФОРМАТИКА, русский язык

24 чел.

Входит в «Перечень специальностей и направлений подготовки высшего образования, соответствующих приоритетным направлениям модернизации и технологического развития российской экономики» (распоряжение Правительства Российской Федерации от 6 января 2015 г. N 7-р).

Новые дисциплины за последние 5 лет

- ✓ Мобильные операционные системы
- ✓ Методы алгебраической геометрии в криптографии
- ✓ Математические аппарат и средства анализа безопасности программного обеспечения
- ✓ Анализ безопасности протоколов
- ✓ Анализ рисков информационной безопасности
- ✓ Мониторинг безопасности информационных систем
- ✓ Методы анализа данных и естественно-языковых текстов
- ✓ Лингвистическое обеспечение автоматизированных систем
- ✓ Безопасность современных высокопроизводительных систем
- ✓ Методы обнаружения и предотвращения вторжений
- ✓ Верификация безопасности информационных систем
- ✓ Теория и системы управления информационной безопасностью
- ✓ Сетевая инфраструктура на основе технологии программно-конфигурируемых сетей

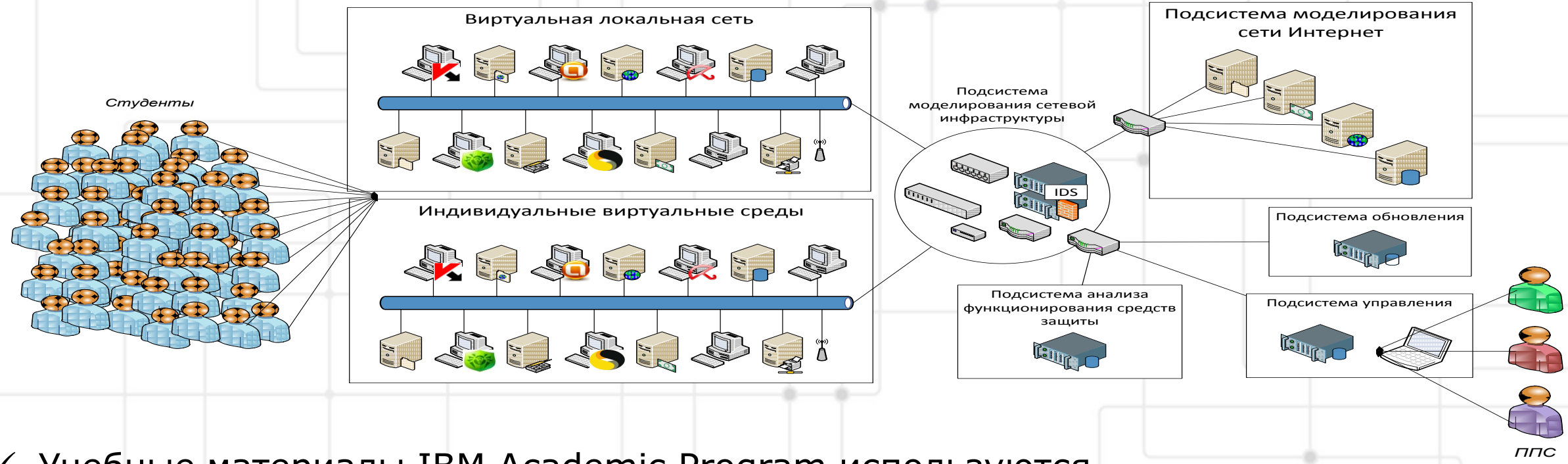
Учебно-методические пособия

Лабораторное обеспечение образовательного процесса

<table>
<tr><th colspan="2">10.05.01– Компьютерная безопасность</th></tr>
<tr><td>Теория управления информационной безопасностью</td><td>Имитационное моделирование гетерогенных распределенных информационно-телекоммуникационных систем</td></tr>
<tr><td>Теория обнаружения и предотвращения вторжений</td><td>Учебные (игровые) сценарии компьютерных атак и противодействия в виртуальных вычислительных средах</td></tr>
<tr><td>Безопасность современных высокопроизводительных систем</td><td>Учебные макеты систем облачных вычислений, грид-систем, систем параллельных вычислений</td></tr>
<tr><th colspan="2">10.05.03– Информационная безопасность автоматизированных систем</th></tr>
<tr><td>Верификация безопасности информационных систем</td><td>Виртуальные информационные системы, операционные системы, распределенные системы</td></tr>
<tr><td>Анализ безопасности протоколов</td><td rowspan="3">Высокопроизводительные системы поиска нарушений безопасности и уязвимостей с помощью параметрического фаззинга и анализа данных мониторинга</td></tr>
<tr><td>Анализ безопасности программного обеспечения</td></tr>
<tr><td>Мониторинг безопасности информационных систем</td></tr>
</table>

ВИРТУАЛЬНЫЕ ТЕХНОЛОГИИ И ДИСТАНЦИОННОЕ ОБРАЗОВАНИЕ

Виртуальная учебная лаборатория



- ✓ Учебные материалы IBM Academic Program используются в учебных дисциплинах «Операционные системы», «Безопасность операционных систем», «Безопасность современных высокопроизводительных систем»
- ✓ Преподаватели прошли обучение в IBM и у партнеров IBM, имеют сертификаты серии “z/OS and OS/390 facilities”

Виртуальная лаборатория

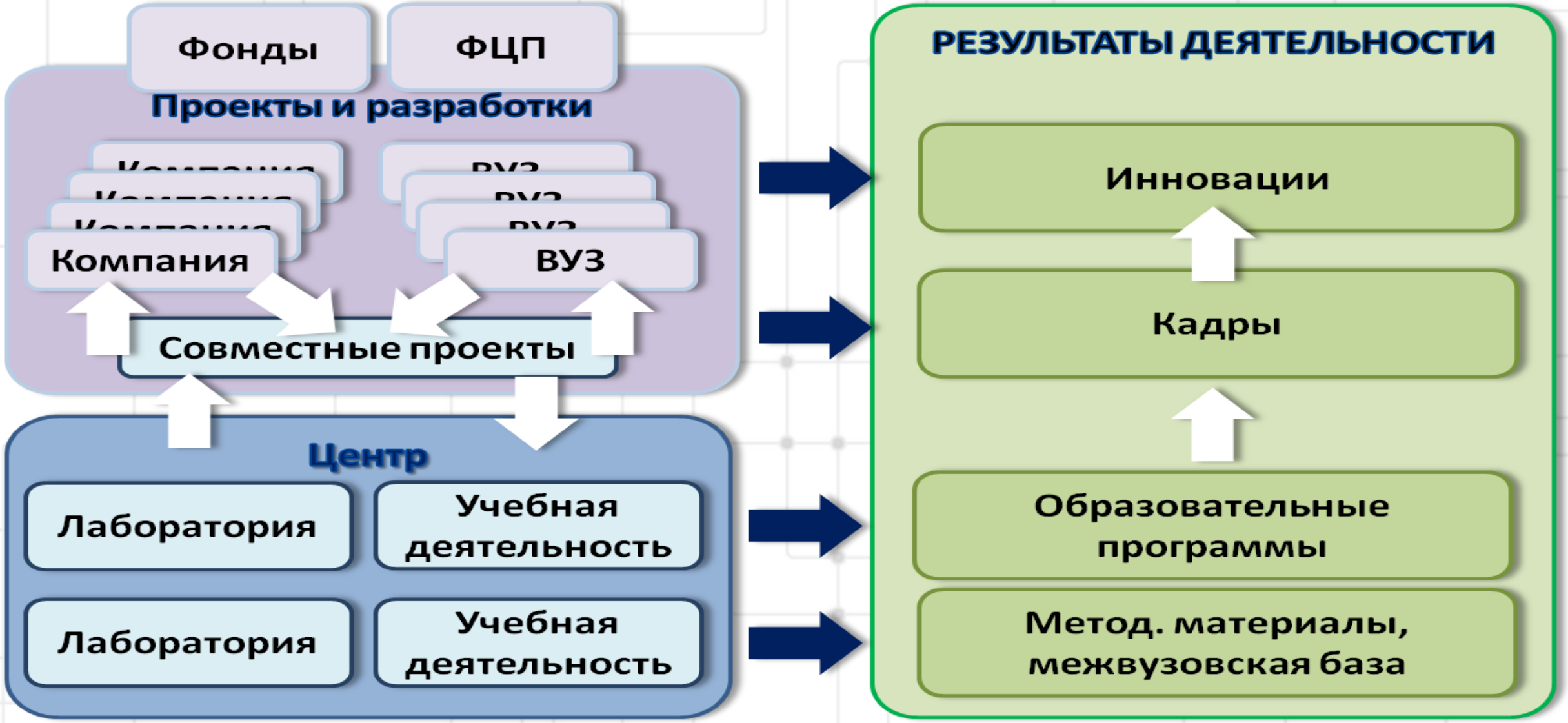
- ✓ является универсальным инструментом для развития дистанционного образования в сфере информационной безопасности.
- ✓ служит практической площадкой – инкубатором технологий, на базе которого студентами отрабатываются идеи и ноу-хау, разрабатываемые в рамках НИР, практики, прогоняются прототипы инициативных разработок, что способствует привлечению и закреплению молодежи в научных проектах

Виртуальная лаборатория

Вычислительные возможности лаборатории служат единым ресурсом по оценке результативности обучения и используются профессорско- преподавательским составом для загрузки заданий, проверки отчетов студентов, проведения различных форм текущего и итогового контроля (тестирование, проверочные работы).

СОТРУДНИЧЕСТВО С ВЕДУЩИМИ IT-КОМПАНИЯМИ
ОБРАЗОВАНИЕ ЧЕРЕЗ ПОГРУЖЕНИЕ
В ПРОЦЕСС РАЗРАБОТКИ

Интеграция науки, образования, бизнеса



Формы взаимодействия ВУЗа и фирм-работодателей

1) Участие специалистов в ГАК, ГЭК, отзывы на рабочие программы.
2) Целевая (платная) подготовка для студентов, аспирантов и докторантов.
3) Передача техники, ПО, стендов во временное пользование ВУЗу. Организация практик.
4) Создание базовых кафедр в фирмах.
5) Договора о сотрудничестве и рамочном взаимодействии (выполнение НИР, ОКР), партнерство в ФЦП, реализация РИД, поддержка конференций.
6) Международные научно-образовательные центры.

Преимущества интеграции

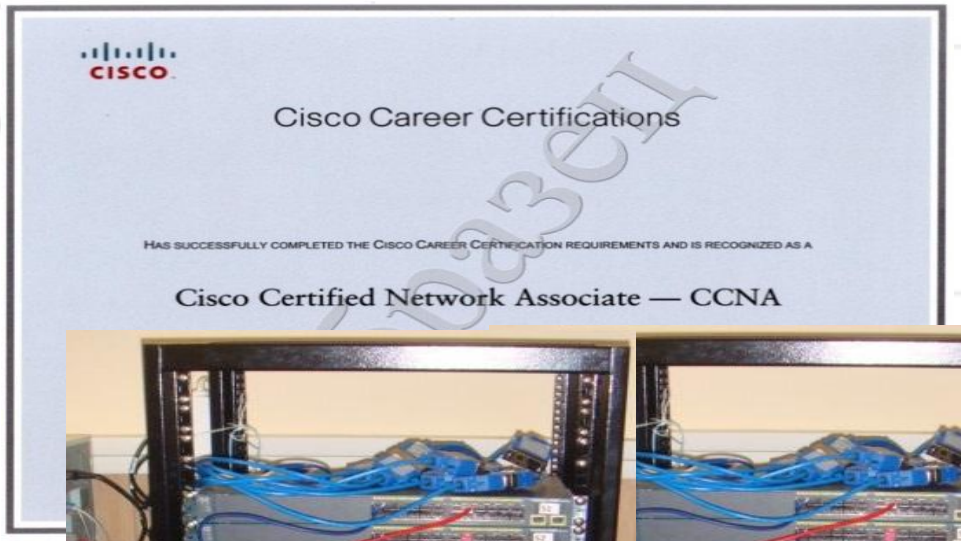
1. **Учёт требований работодателей.**
2. **Сокращение сроков адаптации молодых специалистов.**
3. **Создание условий для повышения квалификации сотрудников фирмы.**
4. **Возможность адаптации учебного процесса к потребностям фирм.**
5. **Балансировка потребностей фирмы и выпуска.**
6. **Возможность подготовки специалистов по комплексу специальностей, т.н. «десантная подготовка».**
7. **Повышение успеваемости за счет заинтересованности студентов.**

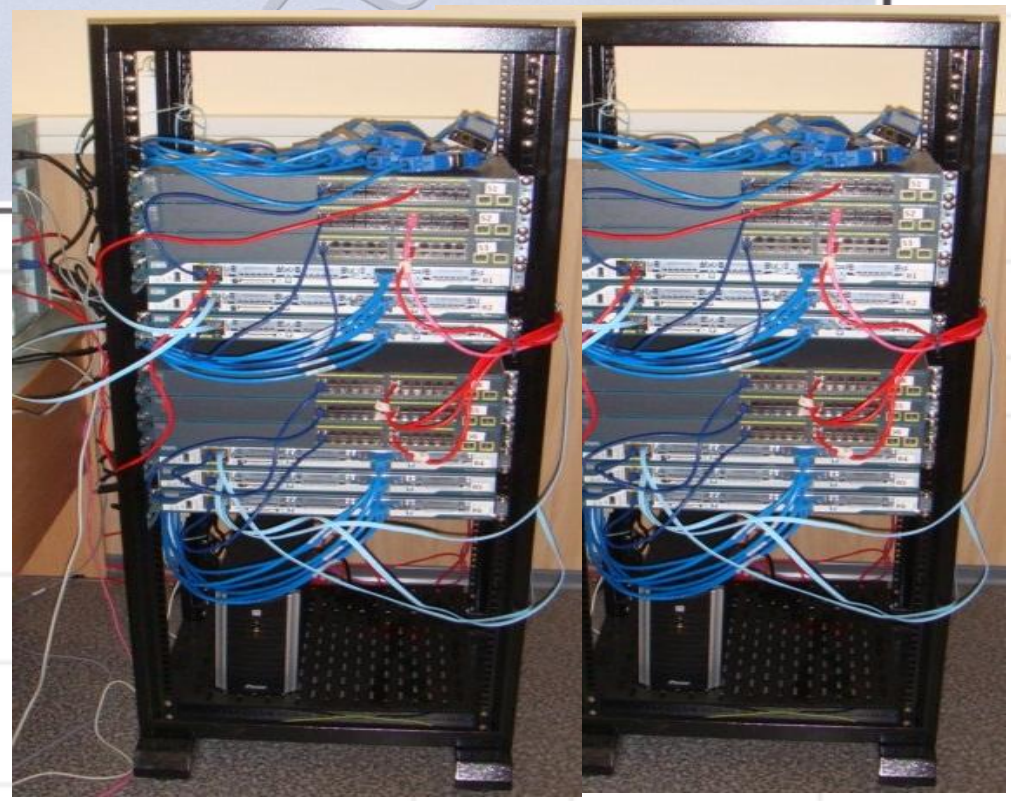
Академия CISCO

С 01.09.2012 г. в рамках учебной программы Академии Cisco обучается более 150 человек

Авторизованная программа подготовки для получения профессиональных сертификатов Cisco

- ✓Учебные дисциплины адаптированы к требованиям Академии Cisco
- ✓Преподаватели прошли обучение в Академии Cisco
- ✓Созданы стенды для проведения лабораторных работ
- ✓Сертифицированные материалы лекций, практические лабораторные занятия
- ✓Инструменты оценки знаний и средства отслеживания академических успехов студентов





Концепция CDIO

CDIO = Conceive - Design - Implement - Operate

международный проект *по реформированию инженерного образования*, начатый в октябре 2000 года в Массачусетском технологическом институте при участии ведущих ученых, преподавателей и представителей промышленности.

Планировать – Проектировать – Производить – Применять

(*www.cdio.org*)

Ключевые идеи CDIO

Цель - приведение содержания и результативности инженерных образовательных программ в соответствие с уровнем развития современных технологий и ожиданиями работодателей.

- **Разрешить противоречие между фундаментальной и практической подготовкой при ограниченном времени обучения**

- **Продемонстрировать на практике важность и применимость полученных знаний, связи между отдельными дисциплинами**

Ежегодное мероприятие по кибербезопасности «NeoQUEST»

http://neoquest.ru

Заочный этап

- Заочный этап длится неделю
- Участвовать могут все желающие
- Участники проходят задания удаленно
- Лучшие участники приглашаются на очный этап

Очный этап

Мероприятие длится один день, вход свободный

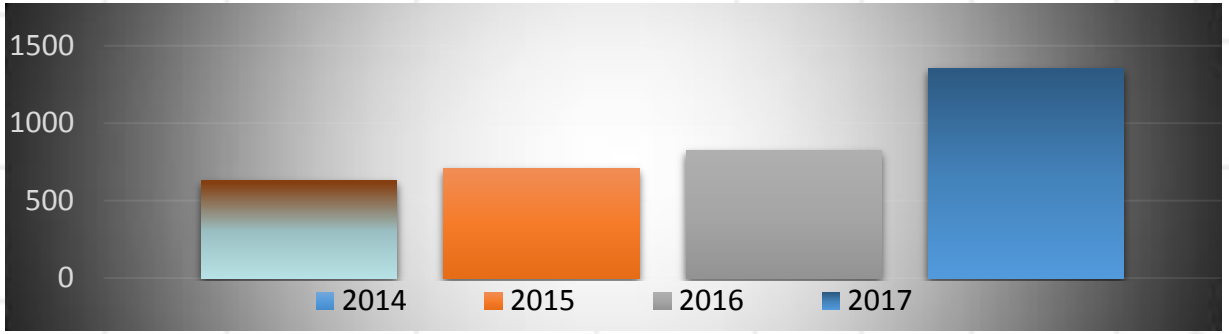
Для гостей мероприятия:

- Доклады и мастерклассы
- Конкурсы и викторина «ЕГЭ по ИБ»

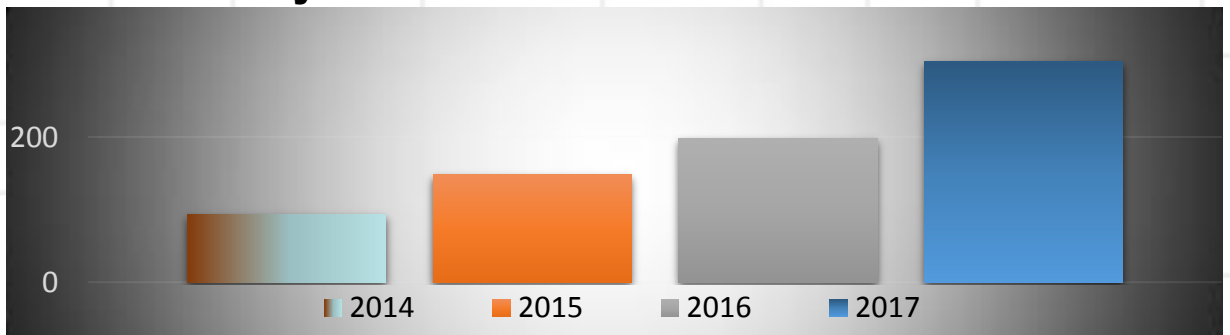
Для лучших участников заочного этапа:

- Соревнование по кибербезопасности

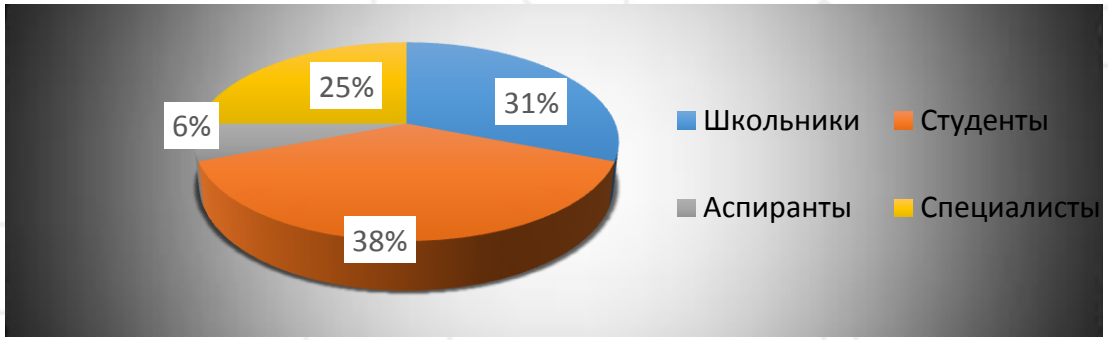
Количество участников в заочных этапах «NeoQUEST»



Количество участников в очных этапах «NeoQUEST»



Процент участия в заочном и очном этапах «NeoQUEST-2017»



AUT VIAM INVENIAM, NEOQUEST AUT FACIAM

Кафедра
«Информационная безопасность компьютерных систем»

Политехническая ул., 29, Главное здание, ауд. 173,
тел: +7(812) 552-64-89, 552-76-32

Web: http://ibks.ftk.spbstu.ru e-mail: kafedra@ibks.spbstu.ru