ЦЕНТР УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ СЛОЖНЫХ СИСТЕМ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ НАУКИ
ИНСТИТУТ ПРОБЛЕМ УПРАВЛЕНИЯ
ИМ. В.А. ТРАПЕЗНИКОВА
РОССИЙСКОЙ АКАДЕМИИ НАУК

СТРАТЕГИЯ НАУЧНО-ТЕХНОЛОГИЧЕСКОГО РАЗВИТИЯ РФ

(утверждена Указом Президента РФ от 01.12.2016 № 642)

Определяет:

наиболее значимые большие вызовы (ст.15):

«а) исчерпание возможностей экономического роста России, основанного на экстенсивной эксплуатации сырьевых ресурсов, на фоне **формирования цифровой экономики** …;

…

е) новые **внешние угрозы национальной безопасности** …, обусловленные ростом международной конкуренции и конфликтности, глобальной и региональной нестабильностью, и усиление их взаимосвязи с **внутренними угрозами национальной безопасности**;»

приоритеты научно-технологического развития (ст.20):

«а) переход к передовым **цифровым интеллектуальным производственным технологиям**, **роботизированным системам**, …, создание **систем обработки больших объемов данных**, **машинного обучения** и **искусственного интеллекта**;

…

д) противодействие **техногенным**, **биогенным**, **социокультурным угрозам**, **терроризму** и **идеологическому экстремизму**, а также **киберугрозам** и **иным источникам опасности** для общества, экономики и государства;»

Подчеркивает, что (ст.21):

«… **Поддержка фундаментальной науки, как системообразующего института долгосрочного развития нации является первоочередной задачей государства**»

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА И ГОСУДАРСТВА

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА И ГОСУДАРСТВА – КЛЮЧЕВОЙ ЭЛЕМЕНТ РАЗВИТИЯ СТРАНЫ В ЦИФРОВУЮ, ИНФОРМАЦИОННУЮ ЭПОХУ

Стратегия национальной безопасности РФ
(утверждена Указом Президента РФ от 31.12.2015 № 683)

УКАЗ
ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О Стратегии национальной безопасности Российской Федерации

В соответствии с федеральными законами от 28 декабря 2010 г. № 390-ФЗ "О стратегическом планировании в Российской Федерации" постановляю:
1. Утвердить прилагаемую Стратегию национальной безопасности Российской Федерации.
2. Признать утратившим силу Указ Президента Российской Федерации от 12 мая 2009 г. № 537 "О Стратегии национальной безопасности Российской Федерации до 2020 года".
3. Настоящий Указ вступает в силу со дня его официального опубликования.

Москва, Кремль
31 декабря 2015 г.
№ 683

Доктрина информационной безопасности РФ
(утверждена Указом Президента РФ от 05.12.2016 № 646)

УКАЗ
ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

Об утверждении Доктрины информационной безопасности Российской Федерации

Указ Президента РФ от 05.12.2016 № 31с **О создании ГосСОПКА**

УКАЗ
ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Указ Президента РФ от 22.12.2017 № 620
О совершенствовании ГосСОПКА

УКАЗ
ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Стратегия развития информационного общества в РФ на 2017 – 2030 годы
(утверждена Указом Президента РФ от 09.05.2017 № 203)

УКАЗ
ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы

В целях обеспечения условий для формирования Федерации общества знаний п о с т а н о в л я ю:
1. Утвердить прилагаемую Стратегию информационного общества в Российской на 2017 - 2030 годы.
2. Правительству Российской Федерации утвердить 2017 г. перечень показателей реализации Стратегии информационного общества в Российской на 2017 - 2030 годы (далее - Стратегия) и план ее реализации
3. Правительству Российской Федерации в 6-месячный
а) внести изменения в документы стратегического в соответствии со Стратегией;
б) обеспечить внесение изменений в документы планирования федеральных органов исполнительной в соответствии со Стратегией.
4. Рекомендовать органам государственной власти Российской Федерации и органам местного самоуправления изменения в документы стратегического в соответствии со Стратегией.
5. Признать утратившей силу Стратегию информационного общества в Российской Федерации Президентом Российской Федерации 7 февраля 2008 г.

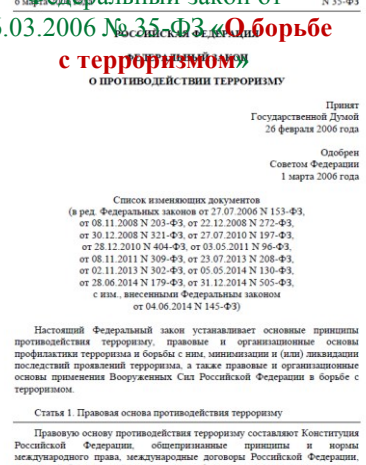
Стратегия экономической безопасности РФ на период до 2030 года
(утверждена Указом Президента РФ от 13.05.2017 № 208)

УКАЗ
ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральный закон от 26.07.2017 № 187-ФЗ «**О безопасности критической информационной инфраструктуры РФ**»

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН

Федеральный закон от 06.03.2006 № 35-ФЗ «**О борьбе с терроризмом**»



РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН
О ПРОТИВОДЕЙСТВИИ ТЕРРОРИЗМУ

Принят Государственной Думой 26 февраля 2006 года
Одобрен Советом Федерации 1 марта 2006 года

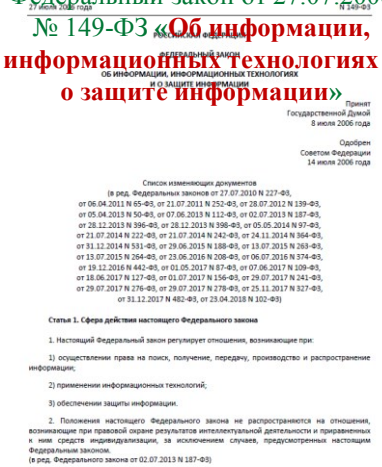
Список изменяющих документов
(в ред. Федеральных законов от 27.07.2006 N 153-ФЗ, от 08.11.2008 N 203-ФЗ, от 22.12.2008 N 272-ФЗ, от 30.12.2008 N 321-ФЗ, от 27.07.2010 N 197-ФЗ, от 28.12.2010 N 404-ФЗ, от 03.05.2011 N 96-ФЗ, от 08.11.2011 N 309-ФЗ, от 23.07.2013 N 208-ФЗ, от 02.11.2013 N 302-ФЗ, от 05.05.2014 N 130-ФЗ, от 28.06.2014 N 179-ФЗ, от 31.12.2014 N 505-ФЗ, с изм., внесенными Федеральным законом от 04.06.2014 N 145-ФЗ)

Настоящий Федеральный закон устанавливает основные принципы противодействия терроризму, правовые и организационные основы профилактики терроризма и борьбы с ним, минимизации и (или) ликвидации последствий проявлений терроризма, а также правовые и организационные основы применения Вооруженных Сил Российской Федерации в борьбе с терроризмом.

Статья 1. Правовая основа противодействия терроризму

Правовую основу противодействия терроризму составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, настоящий Федеральный закон и другие федеральные законы, нормативные правовые акты Президента Российской Федерации, нормативные правовые акты Правительства Российской Федерации, а также принимаемые в соответствии с ними нормативные правовые акты других федеральных органов государственной власти.

Федеральный закон от 27.07.2006 № 149-ФЗ «**Об информации, информационных технологиях и о защите информации**»



РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН
ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ

Принят Государственной Думой 8 июля 2006 года
Одобрен Советом Федерации 14 июля 2006 года

Список изменяющих документов
(в ред. Федеральных законов от 27.07.2010 N 227-ФЗ, от 06.04.2011 N 65-ФЗ, от 21.07.2011 N 252-ФЗ, от 28.07.2012 N 139-ФЗ, от 05.04.2013 N 50-ФЗ, от 07.06.2013 N 112-ФЗ, от 02.07.2013 N 187-ФЗ, от 28.12.2013 N 396-ФЗ, от 28.12.2013 N 398-ФЗ, от 05.05.2014 N 97-ФЗ, от 21.07.2014 N 222-ФЗ, от 21.07.2014 N 242-ФЗ, от 24.11.2014 N 364-ФЗ, от 31.12.2014 N 531-ФЗ, от 29.06.2015 N 188-ФЗ, от 13.07.2015 N 263-ФЗ, от 13.07.2015 N 264-ФЗ, от 23.06.2016 N 208-ФЗ, от 06.07.2016 N 374-ФЗ, от 19.12.2016 N 442-ФЗ, от 01.05.2017 N 87-ФЗ, от 07.06.2017 N 109-ФЗ, от 18.06.2017 N 127-ФЗ, от 01.07.2017 N 156-ФЗ, от 29.07.2017 N 241-ФЗ, от 29.07.2017 N 276-ФЗ, от 29.07.2017 N 278-ФЗ, от 25.11.2017 N 327-ФЗ, от 31.12.2017 N 482-ФЗ, от 23.04.2018 N 102-ФЗ)

Статья 1. Сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, возникающие при:
1) осуществлении права на поиск, получение, передачу, производство и распространение информации;
2) применении информационных технологий;
3) обеспечении защиты информации.
2. Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации, за исключением случаев, предусмотренных настоящим Федеральным законом.
(в ред. Федерального закона от 02.07.2013 N 187-ФЗ)

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

В настоящем Федеральном законе используются следующие основные понятия:
1) информация - сведения (сообщения, данные) независимо от формы их представления;

ЦЕНТР УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ СЛОЖНЫХ СИСТЕМ

Задача:

выстраивание полной инновационной цепочки от создания фундаментального задела до коммерциализации технологий и адресной подготовки специалистов

Направление деятельности:

фундаментальные и прикладные исследования и разработки моделей, методов и технологий управления безопасностью сложных систем

Участники:

- лаборатории ИПУ РАН (20, 31, 46, 49, 57, 77, 79, 80)
- государственные организации (Минобрнауки, Минобороны, МВД, ФСБ, ФСО, ФСТЭК, ГК Росатом и др.)
- научные и образовательные организации (Центр проблем безопасности РАН, МГУ им. М.В. Ломоносова, МГТУ им. Н.Э. Баумана, НИУ ВШЭ и др.)
- промышленные партнеры (Национальная компьютерная корпорация, «Корпорация «Гранит», ГК «Информзащита», НПО «Эшелон» и др.)

Исследовательская основа: виртуальные лаборатории

Инфраструктурная основа: технологические полигоны

НАУЧНО-ТЕХНИЧЕСКИЙ ЗАДЕЛ

ИПУ РАН – ведущее научное учреждение, к основным направлениям научной деятельности которого относятся, в частности:

- **теория систем и общая теория управления**
- **теория управления и методы разработки программно-аппаратных и технических средств управления и сложных информационно-управляющих систем**
- **теория управления безопасностью сложных систем**

ИПУ РАН имеет необходимое количество научных кадров высшей квалификации

140 Докторов наук **250** Кандидатов наук

в том числе обладающих компетенциями в области решения задач обеспечения ИБ объектов КИИ РФ и Цифровой экономики

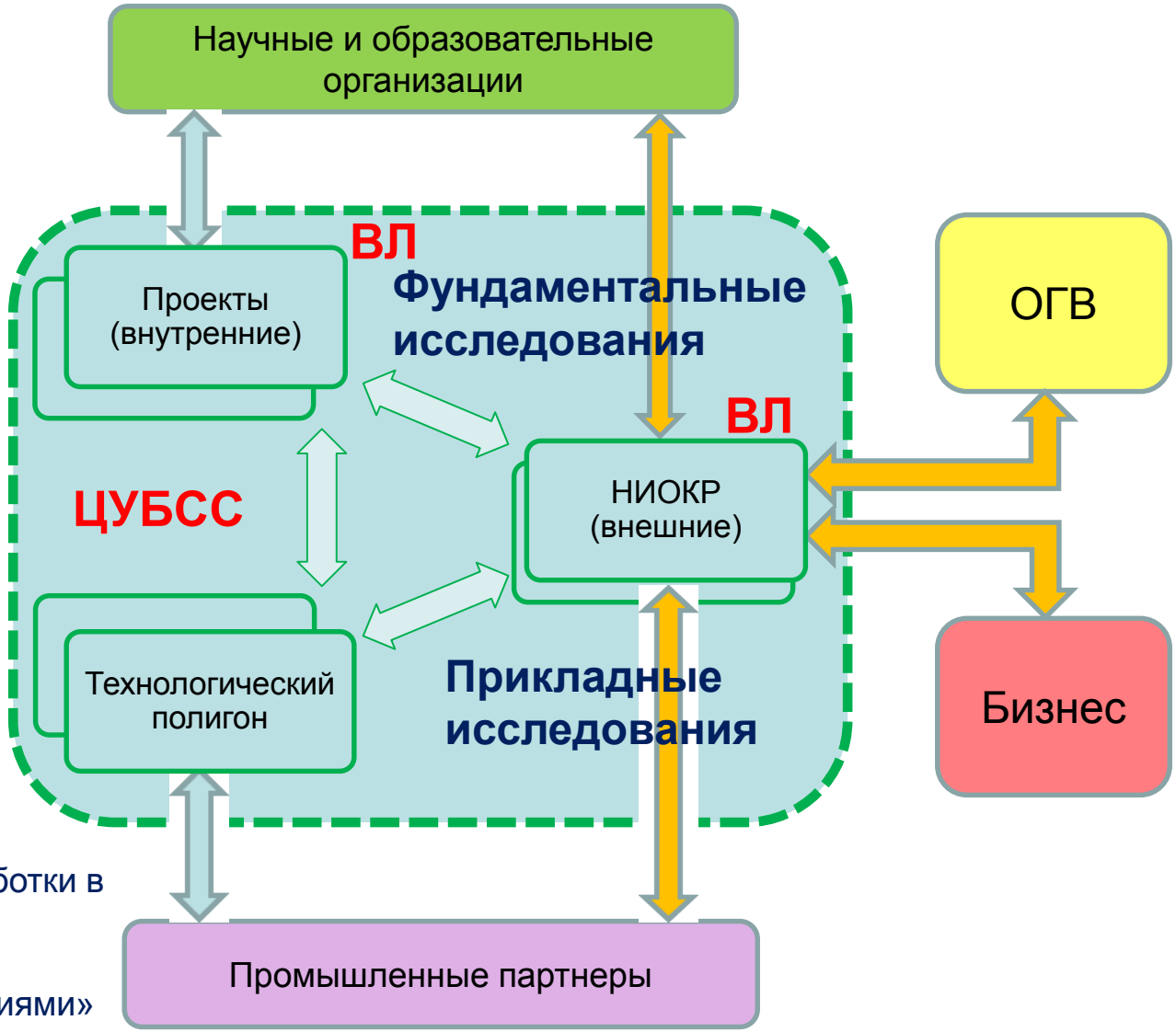
Наличие компетенций подтверждается большим количеством научных публикаций:

более 30 монографий и более 300 статей

ЦЕНТР УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ СЛОЖНЫХ СИСТЕМ: СТРУКТУРА

Лаборатории ИПУ

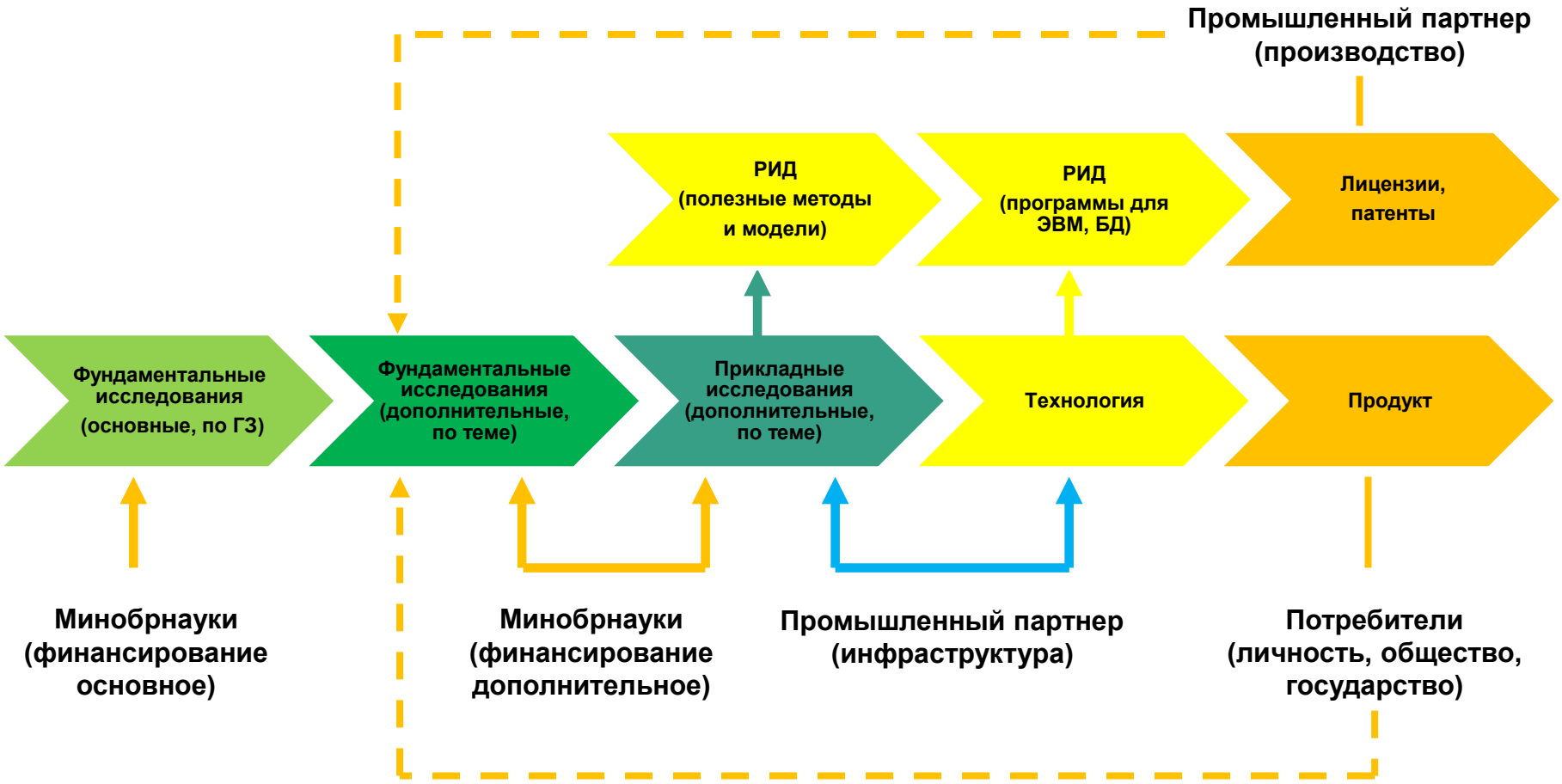
- Лаборатория 20
- Лаборатория 31
- Лаборатория 46
- Лаборатория 49
- Лаборатория 57
- Лаборатория 77
- Лаборатория 79
- Лаборатория 80



Все исследования и разработки в рамках **ЦУБСС** проводятся специально создаваемыми «виртуальными лабораториями» - **ВЛ**

ЦЕНТР УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ СЛОЖНЫХ СИСТЕМ

ПОЛНАЯ ИННОВАЦИОННАЯ ЦЕПОЧКА



ЦЕЛИ ЦЕНТРА НА БЛИЖАЙШУЮ ПЕРСПЕКТИВУ

Цели: фундаментальные и прикладные исследования и разработка моделей, методов и технологий управления безопасностью

СЛОЖНЫХ СИСТЕМ С СЕТЕВОЙ СТРУКТУРОЙ (C^4)

СТРУКТУРА ЗАДАЧ ЦЕНТРА

Фундаментальные задачи управления безопасностью C^4:

- **ИДЕНТИФИКАЦИЯ** объектов;
- **МОДЕЛИРОВАНИЕ** деятельности объектов;
- **ВЫЯВЛЕНИЕ АНОМАЛИЙ** в деятельности объектов;
- **ПРОГНОЗИРОВАНИЕ** развития ситуации.

НЕ ЗАВИСЯТ ОТ ОБЛАСТИ ПРИМЕНЕНИЯ

Прикладные и технологические задачи управления безопасностью C^4:

- **ПАРАМЕТРИЗАЦИЯ** информационного пространства;
- **КЛАССИФИКАЦИЯ** объектов информационного пространства;
- **ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ** по управлению безопасностью;
- **РАЗРАБОТКА** алгоритмического и программного обеспечения.

ЗАВИСЯТ ОТ ОБЛАСТИ ПРИМЕНЕНИЯ

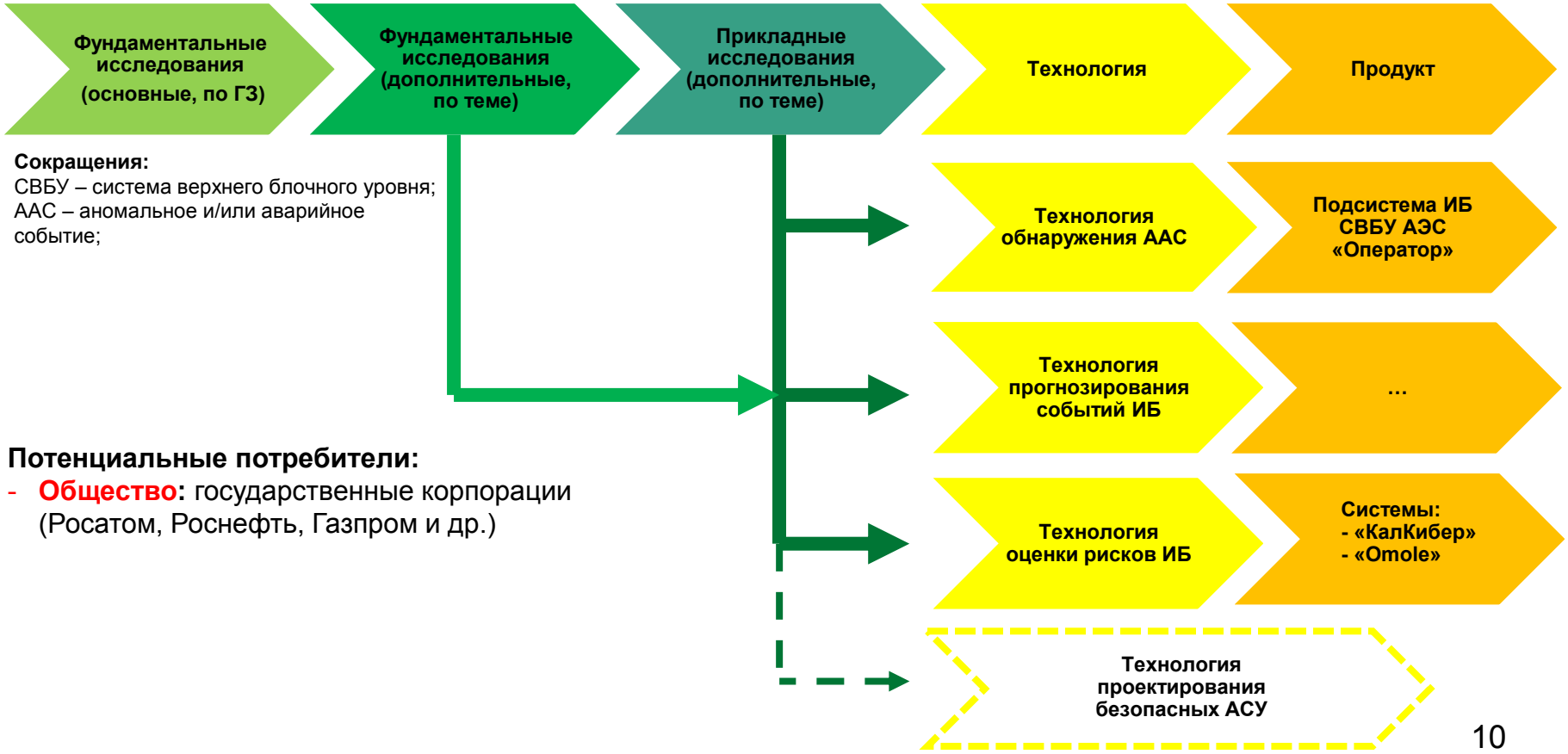
ЗАДАЧИ ЦЕНТРА НА БЛИЖАЙШУЮ ПЕРСПЕКТИВУ:

ТЕХНОЛОГИЧЕСКИЕ СЕТИ

Модели и методы:
- **Идентификации**
- **Моделирования**
- **Выявления аномалий**
- **Прогнозирования**

Модели и методы:
- **Параметризации**
- **Классификации**
- **ППР**
- **Разработка АПО**

Промышленный партнер:
ГК «Росатом»



Сокращения:
СВБУ – система верхнего блочного уровня;
ААС – аномальное и/или аварийное событие;

Потенциальные потребители:
- **Общество:** государственные корпорации (Росатом, Роснефть, Газпром и др.)

ЗАДАЧИ ЦЕНТРА НА БЛИЖАЙШУЮ ПЕРСПЕКТИВУ:

КИБЕРФИЗИЧЕСКИЕ СЕТИ

Модели и методы:
- **Идентификации**
- **Моделирования**
- **Выявления аномалий**
- **Прогнозирования**

Модели и методы:
- **Параметризации**
- **Классификации**
- **ППР**
- **Разработка АПО**

Промышленный партнер:
НКК

Сокращения:
СС – сенсорная сеть;
ЭРР – экстремальный режим работы;
КБ – комплексная безопасность;

Потенциальные потребители:
- **Общество:** государственные корпорации (Росатом, Роснефть, Газпром, Россети и др.); операторы связи (Ростелеком) и др.;
- **Государство:** ФСБ России, ФСО России, ФСТЭК России, МВД России, Росгвардия и др.

ЗАДАЧИ ЦЕНТРА НА БЛИЖАЙШУЮ ПЕРСПЕКТИВУ:

КИБЕРНЕТИЧЕСКИЕ СЕТИ

Модели и методы:
- **Идентификации**
- **Моделирования**
- **Выявления аномалий**
- **Прогнозирования**

Модели и методы:
- **Параметризации**
- **Классификации**
- **ППР**
- **Разработка АПО**

Промышленный партнер:
ФСБ, НКК

Сокращения:
КА – компьютерная атака;
СОВ – система обнаружения вторжений;
ИАО – информационно-аналитическое обеспечение;
НКЦКИ – Национальный координационный центр по компьютерным инцидентам;

Потенциальные потребители:
- **Личность:** граждане РФ – владельцы мобильных устройств;
- **Общество:** государственные корпорации (Росатом, Роснефть, Газпром и др.), заинтересованные в создании корпоративных сегментов ГосСОПКА; организации финансовой сферы (Центральный банк, Внешэкономбанк, Банк ВТБ и др.), заинтересованные в создании корпоративных сегментов ГосСОПКА; операторы связи (Ростелеком), и иные владельцы и собственники объектов КИИ РФ и др.;
- **Государство:** ФСБ России, ФСО России, ФСТЭК России, МВД России, Росгвардия; ФОИВ, заинтересованные в создании ведомственных сегментов ГосСОПКА и др.

ЗАДАЧИ ЦЕНТРА НА БЛИЖАЙШУЮ ПЕРСПЕКТИВУ:

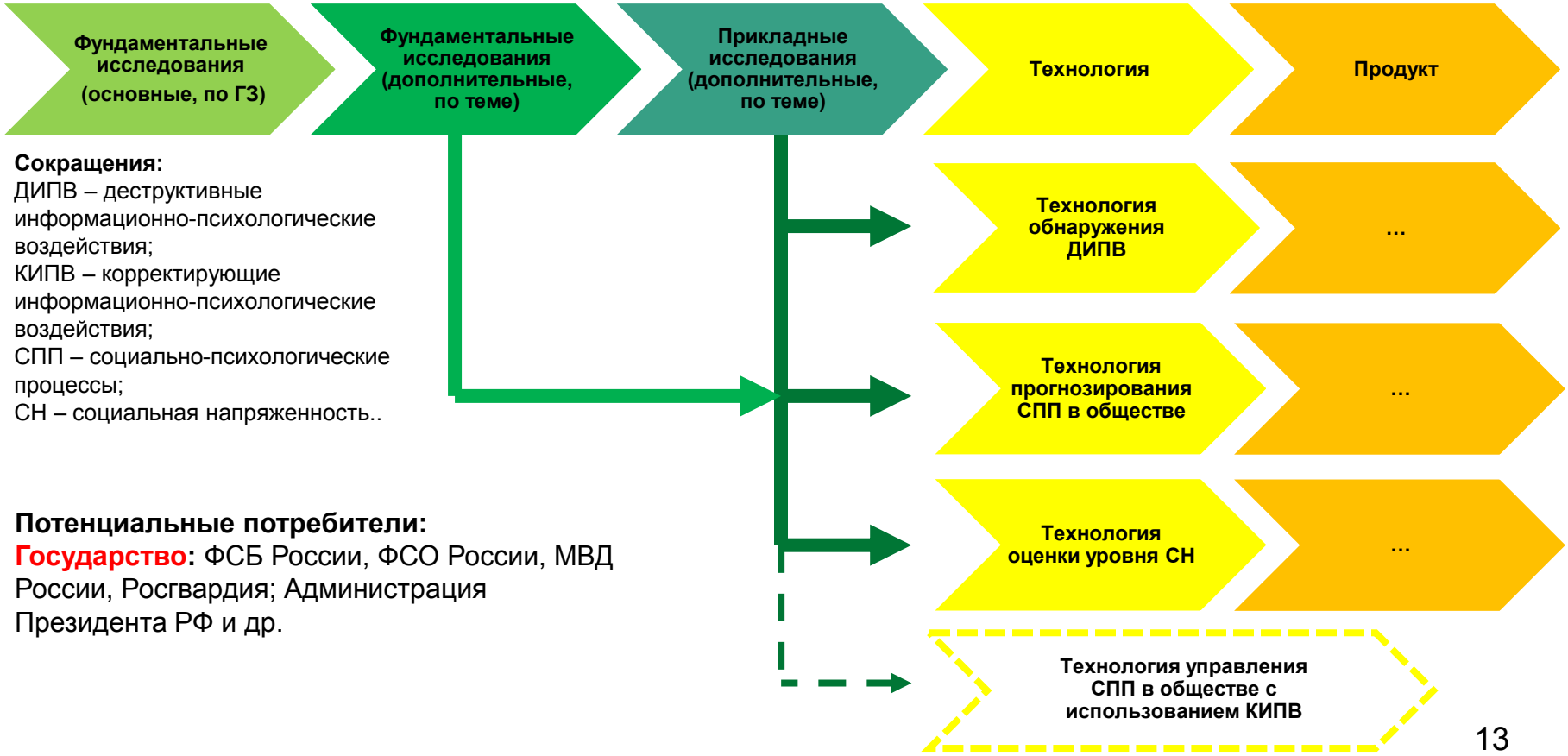
СОЦИАЛЬНЫЕ СЕТИ

Модели и методы:
- **Идентификации**
- **Моделирования**
- **Выявления аномалий**
- **Прогнозирования**

Модели и методы:
- **Параметризации**
- **Классификации**
- **ППР**
- **Разработка АПО**

Промышленный партнер: НКК

Научно-образовательные партнеры: НОЦ ПУ (Воронеж, Пермь, Самара, Волгоград и др.)



Сокращения:
ДИПВ – деструктивные информационно-психологические воздействия;
КИПВ – корректирующие информационно-психологические воздействия;
СПП – социально-психологические процессы;
СН – социальная напряженность..

Потенциальные потребители:
Государство: ФСБ России, ФСО России, МВД России, Росгвардия; Администрация Президента РФ и др.

НАУЧНО-ТЕХНИЧЕСКИЙ ЗАДЕЛ (1)

ИПУ РАН имеет успешный опыт выполнения работ в области моделирования и прогнозирования процессов обеспечения ИБ сложных систем, в том числе:

- исследование вопросов использования математического аппарата теории управления для решения задач обнаружения и предотвращения компьютерных атак;
- исследование вопросов моделирования и анализа динамических сетевых структур, в том числе, построение комплекса математических моделей анализа и прогноза динамики состояний сети в рамках работ по контролю уровня реальной защищенности от угроз терроризма в информационной сфере;
- исследование вопросов использования математических моделей теории управления для решения задач защиты объектов инфраструктуры облачной информационной среды от компьютерных атак;
- разработка математических методов обнаружения компьютерных атак на основе выявления аномалий трафика в сетях TCP/IP;
- разработка параметрических математических моделей и методов комплексной оценки уровня ИБ и рискового потенциала КИИ РФ, в том числе, алгоритмического и программного обеспечения экспериментального образца автоматизированной системы прогнозирования ситуации в области обеспечения ИБ РФ.

НАУЧНО-ТЕХНИЧЕСКИЙ ЗАДЕЛ (2)

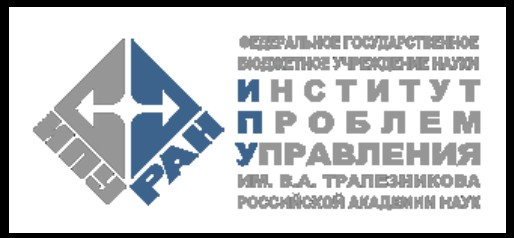
ИПУ РАН реализованы прототипы информационных систем в области моделирования и прогнозирования процессов обеспечения ИБ сложных систем, в том числе:

- комплекс алгоритмического и программного обеспечения для анализа динамики состояний сети;
- комплекс алгоритмического и программного обеспечения экспериментального образца автоматизированной системы прогнозирования ситуации в области обеспечения ИБ РФ;
- комплекс алгоритмического и программного обеспечения реализующего математические методы обнаружения компьютерных атак на основе выявления аномалий трафика в сетях TCP/IP;
- комплекс алгоритмического и программного обеспечения систем управления АЭС, в т.ч. операционная система LICS (Linux Institute of Control Science), разработанная и документированная по российским нормам.

ПОТРЕБИТЕЛИ

Потенциальные потребители результатов ЦУБСС:

- ФСБ России, ФСО России, СВР России, МВД России, Войска национальной гвардии;
- федеральные органы исполнительной власти, заинтересованные в создании ведомственных сегментов ГосСОПКА;
- государственные корпорации (Росатом, Роснефть, Газпром и др.), заинтересованные в создании корпоративных сегментов ГосСОПКА;
- организации финансовой сферы (Центральный банк, Внешэкономбанк, Банк ВТБ и др.), заинтересованные в создании корпоративных сегментов ГосСОПКА;
- операторы связи (Ростелеком), и иные владельцы и собственники объектов КИИ РФ;
- и др.



НАШИ КОНТАКТЫ

Россия, 117997, Москва
ул. Профсоюзная, д. 65

+7 495 334-89-10

dan@ipu.ru

www.ipu.ru