ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСТИТЕТ

ГЛАВНЫЙ
НАУЧНЫЙ ИННОВАЦИОННЫЙ
ВНЕДРЕНЧЕСКИЙ ЦЕНТР
ГНИВЦ

Роль традиционных мер ИБ в защите от КА

АКАДЕМИК АКАДЕМИИ КРИПТОГРАФИИ
А.П. БАРАНОВ
abaranov@hse.ru

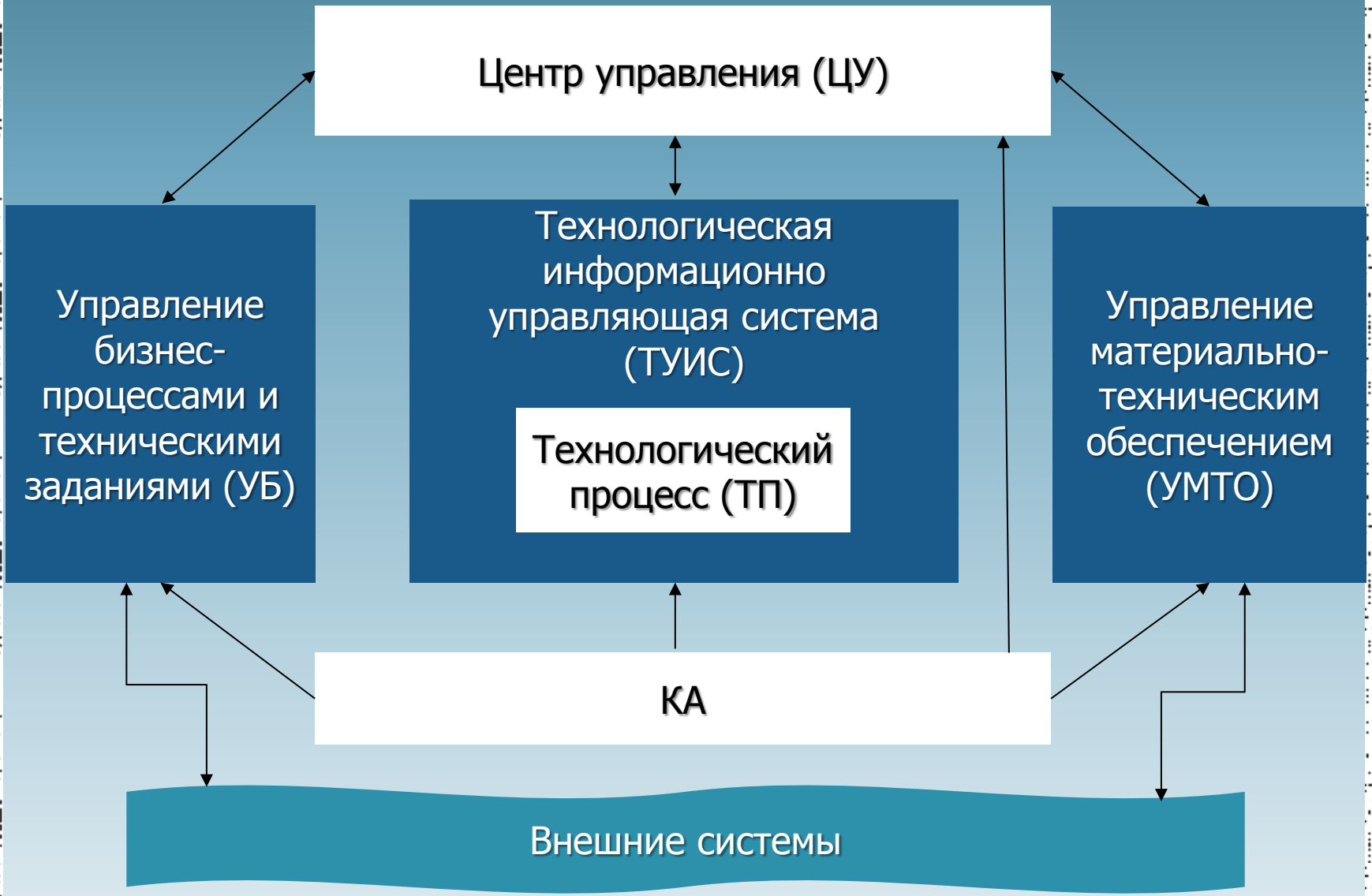
ДОЦЕНТ НИУ ВШЭ
П.А. БАРАНОВ
pbaranov@hse.ru

abaranov@hse.ru, pbaranov@hse.ru

Критическая информационная инфраструктура (КИИ) объекта промышленности и государственно-общественного управления

1. По Закону № 187 от 26.07.2017 объекты КИИ это автоматизированные системы управления основными производственными, экономическими и политическими процессами Российского государства, независимо от форм собственности.
2. Обеспечение безопасности КИИ РФ - обеспечение устойчивого функционирования объектов КИИ при проведении в ее отношении компьютерных атак (КА)
3. КА – целенаправленное воздействие программно-техническими средствами (ПТС) в целях нарушения функционирования или безопасности обрабатываемой ими информации (ИБ)
4. ИБ – конфиденциальность (К), целостность (Ц), доступность (Д)

Общая схема информационной инфраструктуры объекта КИИ



Общая схема производственной ТУИС

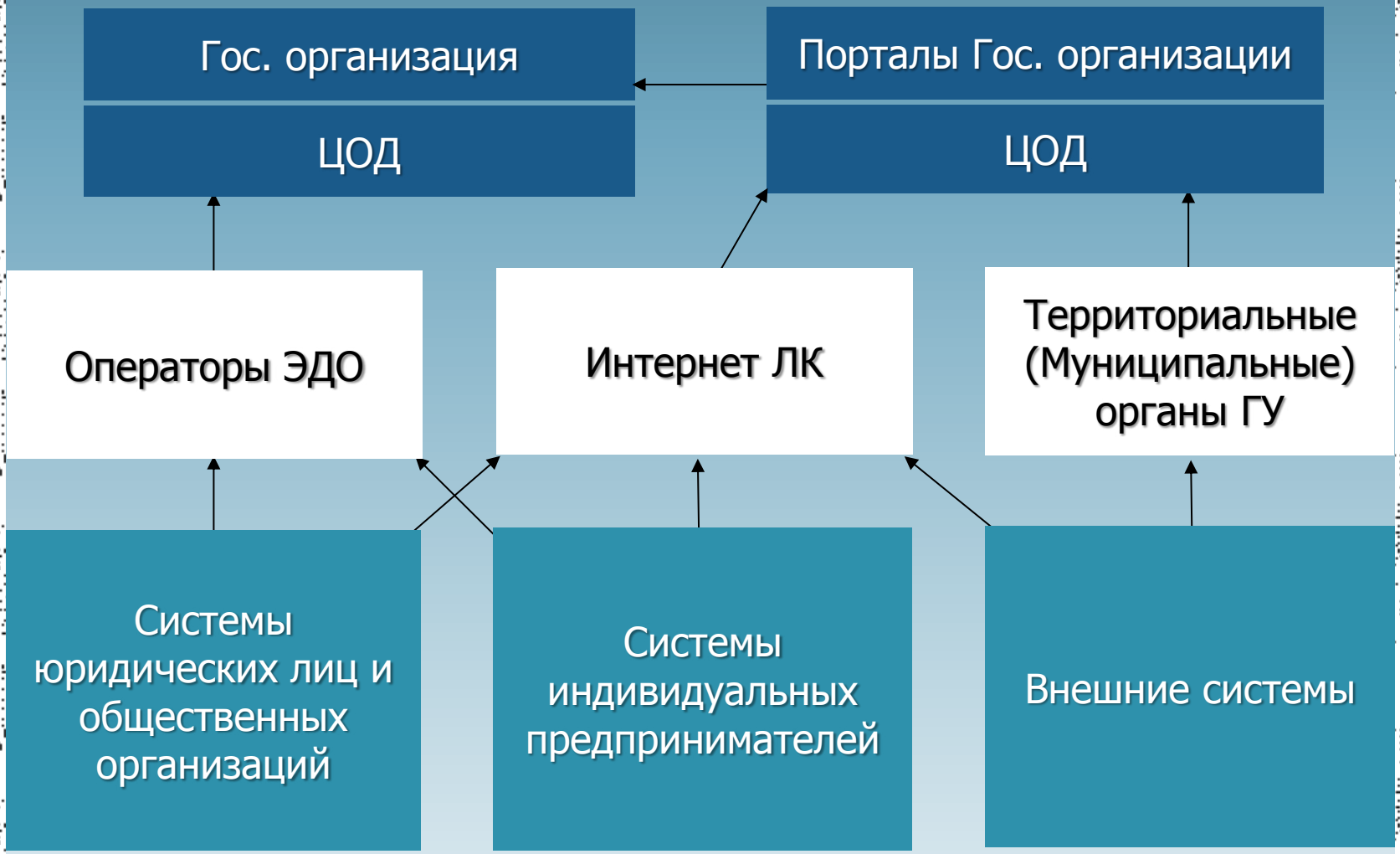
Производственная ЛВС (Совокупность ЛВС)

- Датчики технологических процессов
- Сервера анализа состояния технического процесса и управления
- Система хранения регламентов действий, ПО, логов
- Обеспечение работы ЛВС

ЛВС обеспечения деятельности

- Система Центра доступа
- Система пожаротушения
- Контроль энерго обеспечения
- Система климатических параметров
- ...

Общая схема ТУИС госуправления
Массовые системы



abaranov@hse.ru, pbaranov@hse.ru

Массовые технические системы, привлекательные для КА

1. Целостность локальных ЛВС (автономных датчиков):

   a) домашние системы контроля или безопасности - квартир 6 x 10^7;
   b) автомобили и средства транспорта - 6 x 10^7 ед.;
   c) ККТ и торговые системы - 5 x 10^6;
   d) системы городских хозяйств – 10^4 (городов);
   e) предприятий промышленности – 10^5;

2. Архитектуры ИС близки к стандартной: ЛВС с выходом во вне и в Интернет через FW

3. Массовость требует эффективных, но несложных в эксплуатации и недорогих средств ИБ

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

ИБ и устойчивость ПО к несанкционированному изменению

ГНИВЦ

1. Массовые системы требуют возможности корректного удаленного изменения ПО
2. ИБ требует фиксации ПО. Диалектичное противоречие, как ИБ и широта ППО
3. Что неизменного в ПО? Фирменное ПО датчиков «зашито», не изменяемо и поддается только трудоемкому исследованию
4. ПО серверов анализа и регулирования технических процессов доступно только в исполняемом коде
5. Системы хранения и обеспечения трафика – продукты общего применения
6. Внешнее проникновение в часть системы реализует возможности внутреннего противника

abaranov@hse.ru, pbaranov@hse.ru

Изоляция – действенный метод защиты от внешнего нарушителя

1. Полная (физическая) изоляция крупного объекта от общемировой сети практически невозможна
2. Виртуальная изоляция возможна на основе криптографических протоколов удаленного взаимодействия КС 1-2 или КС 3- КА?
3. Двустороннее взаимодействие с внешней средой необходимо для функционирования УБ и УМТО
4. Массовость систем требует сочетания априорной защиты и апостериорного мониторинга (SIEM)
5. Защита УБ и УМТО требует применения национальных норм и методов, стыкуемых с международными техническими протоколами и правилами. Демилитаризованные зоны сложны

abaranov@hse.ru, pbaranov@hse.ru

Внутренний нарушитель (ВН)

1. Реальность ВН показывает практика как банковской деятельности, так и функционирования органов правопорядка ряда государств. Это особенности человеческой психики
2. Нарушитель характеризуется высокой профессиональной подготовкой в области компьютинга и всеядностью - все до чего дотянулся
3. Возможность отложенной, автономной активизации (управление по ситуации) и высокая скрытность незаконных действий, следовательно защита по КС 3
4. Мониторинг функционирования персонала и состояния КИИ. Неотвратимость наказания и быстрота реакции – основной сдерживающий фактор
5. Юридически значимая фиксация действий персонала

СПАСИБО ЗА ВНИМАНИЕ

abaranov@hse.ru
pbaranov@hse.ru