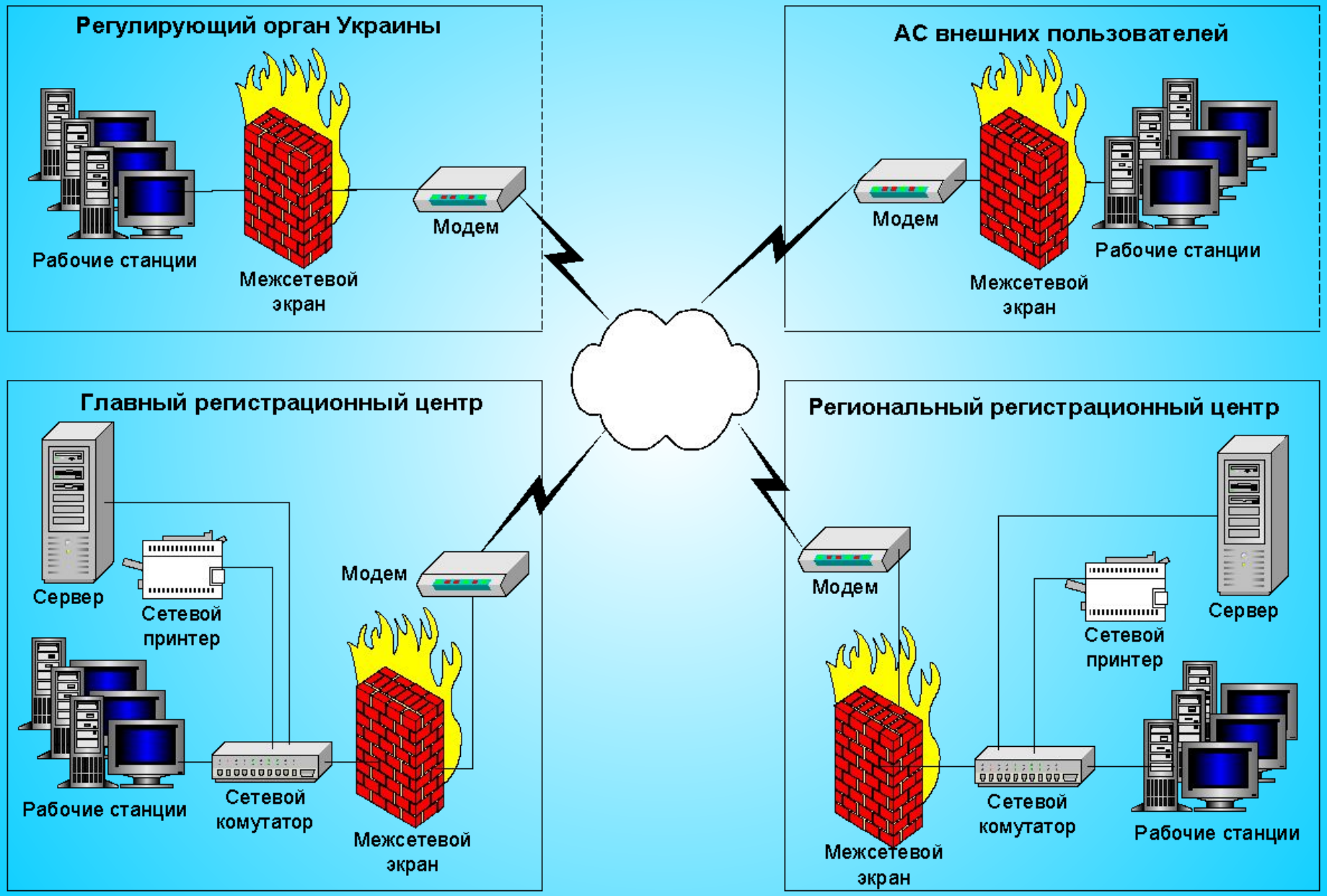
Центр технической защиты информации ОАО «КП ВТИ»

Особенности формирования требований информационной безопасности Реестра источников ионизирующего излучения (ИИИ), которые могут быть использованы с террористической целью

Докладчик - Короленко Михаил Петрович,
начальник центра,
csi@kpvti.kiev.ua, тел. (044) 450 18 43

Обеспечение надежного учета источников ионизирующего излучения (ИИИ), контроля за их местом расположения и перемещением, проведение анализа их количественного и качественного состава, прогнозирование их накопления, объемов их обслуживания, потребности в производственных мощностях предприятий-производителей ИИИ и специализированных предприятий по обращению с радиоактивными отходами требует создания защищенной автоматизированной технологии обработки информации о ИИИ на всех стадиях их жизненного цикла.

Архитектура автоматизированной системы «Регистр»



Инструкция по обеспечению защиты информации Государственного регистра источников ионизирующего излучения разработана в соответствии с требованиями Законов Украины: «Об информации» и «О защите информации в информационно-телекоммуникационных системах», нормативных документов системы технической защиты информации (НД ТЗИ), плана НДДКР Государственного комитета ядерного регулирования, а также на основании анализа технологии обработки информации, анализа рисков для ресурсов Государственного регистра, возможных угроз информации (модели угроз) и требований установленной (принятой) политики безопасности информации.

Разработка Научно-исследовательским информационно-аналитическим центром «ЛЕКС» «Перечня ИИИ, которые могут быть использованы с террористической целью» может привести к пересмотру сформулированных в Инструкции требований к обеспечению защиты информации в Государственном регистре.

Определение правового режима доступа к информации о ИИИ, которые могут быть использованы с террористической целью, потребует рассмотрения вопроса обеспечения безопасности в АС двух категорий информации, требования к защите которых будут существенно отличаться.

Для формирования требований информационной безопасности необходимо:

- Определить правовой режим доступа к информации о ИИИ, которые могут быть использованы с террористической целью;
- Провести классификацию всех информационных ресурсов АС «Регистр» и определить множества информационных объектов, относящихся к различным категориям ограничения доступа;
- Разработать модель угроз с учетом возможного использования злоумышленниками информации Регистра ИИИ для реализации угроз террористических актов;

- Провести классификацию субъектов информационной деятельности по категориям полномочий доступа к различным категориям ресурсов АС;
- Доработать политику безопасности АС Регистр с учетом особенностей требований к технологии обработки различных категорий информации;
- Разработать правила разграничения доступа пользователей к различным категориям информации;
- Разработать правила реагирования на попытки несанкционированного доступа к различным категориям информации;

- Провести анализ достаточности средств защиты и организационных мероприятий для реализации принятой политики безопасности;

- Разработать и реализовать мероприятия по обеспечению реализации принятой политики безопасности;

- Разработать и ввести в действие новую редакцию Инструкции по обеспечению защиты информации Государственного регистра ИИИ.

Комплексные системы защиты информации

Перечень КСЗ, разработанных ОАО «КП ВТИ», в качестве программно-технического ядра построения КСЗИ

КСЗ (платформа)	Класс защищаемой АС	Назначение
«Рубіж РСО» (Windows 2000/XP Pro)	АС класса 1	Предназначен для обеспечения безопасной информационной технологии обработки информации с ограниченным доступом на изолированной РС
«Рубіж 2» (Windows 2000/2003Ser /2000/XP Pro	АС класса 2	Предназначен для обеспечения безопасной информационной технологии обработки информации с ограниченным доступом в локальной вычислительной сети
«Рубіж» (Windows 2000/2003Ser /2000/XP Pro	Средства интеграции защиты в коммуникациях	Предназначен для обеспечения безопасной информационной технологии обработки информации с ограниченным доступом в корпоративной вычислительной сети