Комплексный подход к построению систем защиты информации на критически важных объектах инфраструктуры.

{ арго технолоджи }

комплексные решения
по информационным
технологиям
и защите информации

Компетенции в области информационных технологий и услуг

Тезисы

1. **Краткий обзор актуального состояния защищённости информации ключевых информационных систем в нашей стране;**

2. **Обзор наиболее удачных внедрённых систем информационной безопасности на критически важных объектах инфраструктуры в общемировой практике;**

3. **Предложения по созданию высокоэффективных, универсальных компонент систем защиты информации на критически важных объектах инфраструктуры;**

4. **Концептуальная модель многоуровневой системы защиты информации критически важного объекта инфраструктуры с применением существующих передовых технических решений;**

5. **Ответы на вопросы.**

1. Краткий обзор актуального состояния защищённости информации ключевых информационных систем в нашей стране;

Защита КСИИ – мода или необходимость?

Какие угрозы возможны для КСИИ?

Последствия реализации угроз.

Рассмотрим, как видят проблему создания защиты информации различные заинтересованные стороны…

Взгляд на систему информационной безопасности КСИИ с точек зрения:

Государства

С точки зрения государства, система информационной безопасности КСИИ – это элемент системы управления, связанный с обеспечением безопасности оборудования, разработанный согласно стандартам типа С. Подробно об общих принципах конструирования которых можно узнать из Национального стандарта Российской Федерации ГОСТ Р-ИСО 13849-1-2003.

В ГОСТе – нет требований из РД ФСТЭК. В РД ФСТЭК – не учтены требования ГОСТа.

А значит, созданная по ГОСТу КСИИ – защищена.

Крупного бизнеса

Законодательство в области защиты КСИИ, с точки зрения бизнеса в РФ отсутствует вообще. РД ФСТЭКа воспринимаются как рекомендации, абсолютно не обязательные к исполнению. Мало того, в известном смысле вредные для бизнеса, так как запрет внешних коммуникаций из КСИИ в свою очередь ведёт к нарушению обязательств компании и нарушению ряда законных и подзаконных актов.

А главная проблема это сама постановка вопроса бизнесом – А нужна ли защита вообще?

Производства

<u>Любые средства защиты информации – вредны для процесса производства!</u>

Помимо этого, по требованиям ФСТЭК, КСИИ не может быть объединена с системой низшего класса защиты, то есть всего два пути, либо объединять всё в одну большую КСИИ либо дробить внутри АСУ ТП сегменты, защищённые друг от друга и сами от себя. А это – крайне тяжело осуществить.

Крайне важно разработать систему классификаций КСИИ, и интеграция данной классификации с классификацией АИС, что позволит объединять КСИИ с другими системами, значительно упрощая задачу по разработке элементов информационной защиты.

Компаний - подрядчиков

Под подрядчиками понимаются государственные и частные организации, участвующие в передаче, обработке и консолидировании данных, получаемых от КСИИ, обслуживать которые они взялись, а также разработчики самих систем АСУ ТП, которые встраиваются в КСИИ.

У данной подгруппы проблем несколько:

- Бюджет и внутренняя политика;

- Потеря гарантийных обязательств при внедрении СЗИ.

Ответственность

Однако стоит отметить, что если КСИИ является частью системы управления производственным процессом (согласно ГОСТ Р-ИСО 13849-1-2003) то в случае нарушения её функционирования эксплуатирующие её компании и должностные лица попадают, согласно закону "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях и Федеральный закон ", вступившего в силу с 1 января 2011 года под следующие виды ответственности:

- административные штрафы, дисквалификации, приостановление деятельности,

2. Обзор наиболее удачных внедрённых систем информационной безопасности на критически важных объектах инфраструктуры в общемировой практике;

Какие средства защиты информации использовать в КСИИ?

Согласно руководящим документам ФСТЭК, для защиты КСИИ разрешается использовать СЗИ, подходящие по требованиям для защиты автоматических информационных систем класса 1В.

Основных мнений у экспертов – два:

Одни эксперты настаивают на том, что с учётом постоянно растущего влияние автоматики на производственные процессы необходимо совершенствовать средства защиты информации, разрабатывая специальные, профильные СЗИ встраиваемые в АСУ ТП уже на стадии производства.

Другие же настаивают на консервативном, однако зарекомендовавшем себя подходе к данной проблеме – защите организационно-режимными мерами, с применением наложенных СЗИ.

Неоднозначность мнений вызвана тем, что с одной стороны КСИИ защищать необходимо, и это все понимают. А с другой стороны – выбор специализированных средств защиты информации для КСИИ очень невелик.

Вот несколько сертифицированных промышленных средств защиты информации на сегодняшний день:

- Промышленные межсетевые экраны или промышленные коммутаторы с функциями межсетевого экрана, поддерживающие промышленные протоколы передачи данных (Промышленные коммутаторы Huawei с функциями межсетевого экранирования серии S9300, Промышленный МСЭ StoneGate FW-5205);

Huawei S9300

StoneGate FW-5205

- Системы мониторинга событий информационной безопасности (Системы сбора и корреляции логов RSA envision)

RSA SECURITY

- Системы обнаружения и предотвращения вторжений, поддерживающие промышленные протоколы передачи данных (Высокопроизводительный модуль StoneGate IPS 3205);

STONESOFT
Network Security

- СЗИ от НСД, поддерживающие работы на Сервере Реального Времени. (СЗИ «Diamond ACS»).

СЗИ НСД «Diamond ACS» TSS

Лидерами мирового рынка промышленных средств защиты информации являются компании Industrial Defender, TOFINO, Huawei, Cisco с подобной продукцией которых отечественный рынок почти не знаком.

А учитывая политики конфиденциальности некоторых вендоров (Отказ в предоставлении исходных кодов для проведения сертификационных испытаний) знакомства может и не получиться. Не забываем, что запрет на использование несертифицированных средств защиты в отечественных системах информационной безопасности ещё никто не отменял.

- НДВ есть?
- А если найдём??

Некоторые вендоры, например, Huawei, имеют свой собственный подход к повышению защищённости своих продуктов. Предложенный ими технический подход рассказывает об объединении нескольких механизмов защиты в одном устройстве, причём с возможностью гибкой настройки с единой консоли управления.

Рынок специализированных средств защиты информации предназначенных для АСУ ТП только начал развиваться, но темпы его развития – впечатляют, однако ничего удивительного – спрос на подобную продукцию – растёт, а значит и предложения – не заставят себя ждать.

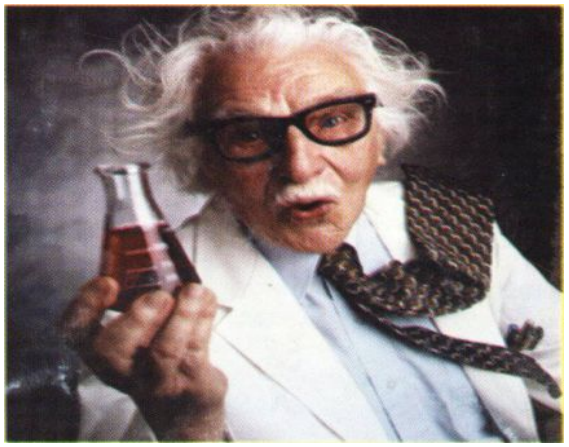
На отечественном рынке положение усугубляется специфичностью требований Органов-регуляторов в части контроля НДВ в изделиях иностранных вендоров. Данное требование резко сокращает ассортимент разрешённых для использования на территории России средств промышленной безопасности. Однако многие иностранные вендоры всё-таки пошли на встречу и позволили провести необходимые обследования своих изделий, что в свою очередь позволило наконец решить вопрос о выборе средств защиты информации для КСИИ.

3. Предложения по созданию высокоэффективных, универсальных компонент систем защиты информации на критически важных объектах инфраструктуры

Подход к созданию систем защиты информации КСИИ – уникален.

Очевидно, что невозможно создать высокопроизводительное, эффективное и полностью универсальное средство защиты, идеально подходящее для любого вида КСИИ.

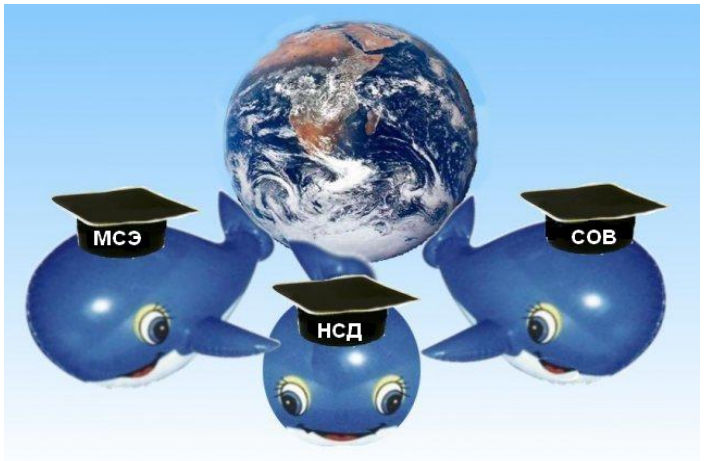
Однако решение данной проблемы существует!



Итак, из каких основных технических средств состоит любая классическая система защиты:

- Средство межсетевого экранирования;
- Средство обнаружения и предотвращения вторжений;
- Средство защиты от НСД;

Это три обязательных кубика в фундаменте любой системы защиты информации.



Закупка средств защиты информации и их сертификация по требованиям ФСТЭК – процедура дорогая и долгая. К тому же покупая средства межсетевого экранирования и средства защиты от НСД, покупатель не может быть уверен в том, что при их совместной работе не возникнет внутрисистемных конфликтов. Так как на совместимость данные средства никто не проверял…

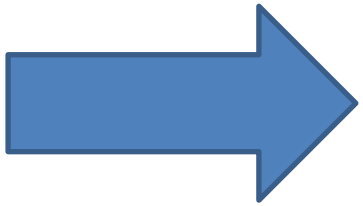
Наша компания организовала производство средств автоматизации в защищённом исполнении, объединяющих два из трёх основных технических средств защиты информации в одно, что поможет избежать дальнейших затрат и позволит избежать накладок с совместимостью.

Мы производим промышленные коммутаторы с функциями межсетевого экранирования и встроенными средствами защиты от НСД. Продукт производится на территории России и имеет все необходимые сертификаты.

Данный процесс выглядит так:

Промышленный коммутатор с функциями межсетевого экрана

+



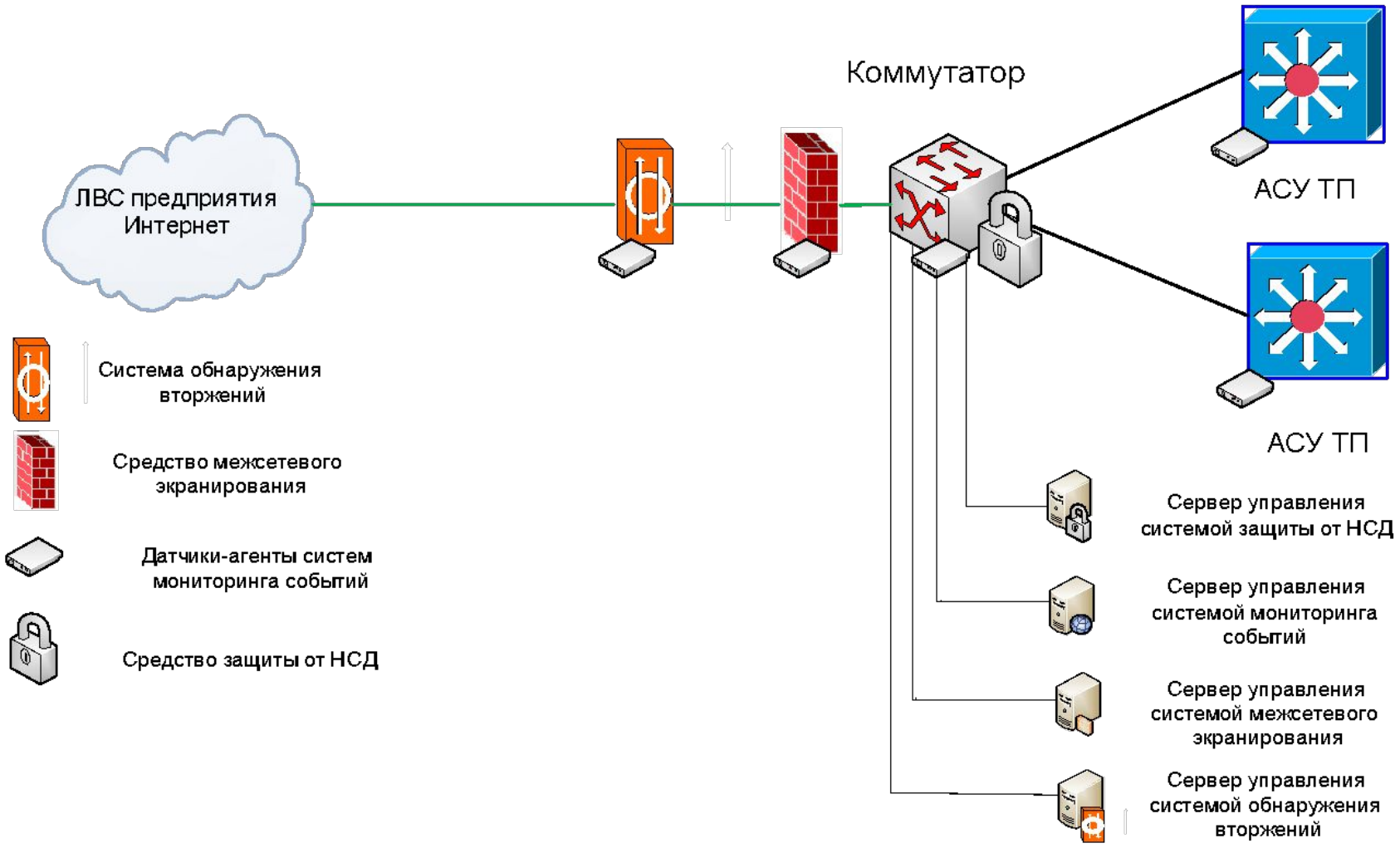
Мультиплатформенное СЗИ от НСД

Сертифицированный межсетевой экран с встроенным средством защиты от НСД на базе промышленного коммутатора

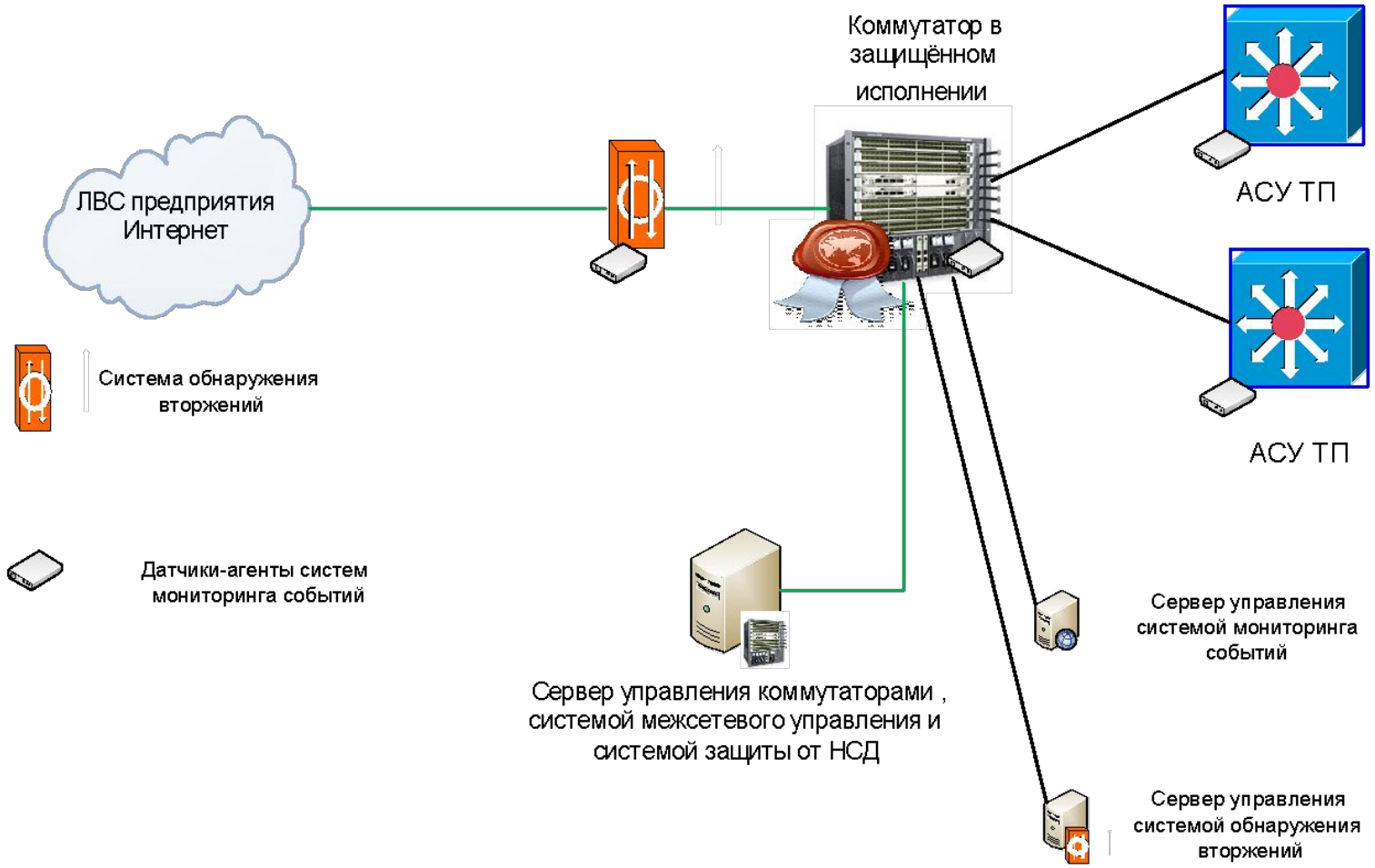
Или Промышленный коммутатор в защищённом исполнении, предназначенный для использования в КСИИ

4. Концептуальная модель многоуровневой системы защиты информации критически важного объекта инфраструктуры с применением существующих передовых технических решений.

1. *Классический подход создания системы защиты информации:*



2. *Создание системы информационной безопасности используя защищённые коммутаторы:*



Преимущества модульного подхода – очевидны!