ICL СИСТЕМНЫЕ ТЕХНОЛОГИИ

РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТОВ КИИ НЕФТЕПЕРЕРАБАТЫВАЮЩЕГО ПРЕДПРИТИЯ

https://icl.ru/

Ирек Азизов
Генеральный директор
ICL Системные технологии

ПРОЕКТ

ICL СИСТЕМНЫЕ ТЕХНОЛОГИИ

Разработка и внедрение системы обеспечения информационной безопасности (СОИБ) для критической информационной инфраструктуры АСУ ТП

**№187-ФЗ от 26.07.2017г.
«О безопасности критической информационной инфраструктуры РФ»**

UserGate

positive technologies

infotecs

kaspersky

СЛОЖНОСТИ

Проблемы, связанные с импортозамещением:

- Функционал решений, на которые были заменены иностранные аналоги, имеет технические недостатки;
- Иностранные компоненты АСУ ТП не проходили тестирование на совместимость с отечественными решениями;
- Отсутствие технической поддержки со стороны используемых решений (заменяемые решения/решения, которые не заменяются и будут взаимодействовать с СОИБ);

В АСУ ТП сегменте используются устаревшие компоненты (например ОС):

- Модернизация невозможна, т.к. другие компоненты технологических систем несовместимы;

Наличие в сегментах АСУ ТП самописного ПО (скриптов), выявленного в ходе ПНР:

- Подобное ПО не декларировалось изначально в проекте, СЗИ начинают его блокировать;

ПУТИ РЕШЕНИЯ

Взаимодействие с вендором внедряемых средств	Обходные технические решения, не предусмотренные изначальным проектом	Организационные компенсирующие меры

РЕЗУЛЬТАТЫ

- Обеспечение соответствия объектов КИИ требованиям законодательства РФ в области обеспечения безопасности объектов КИИ;
- Обеспечение заданного уровня устойчивости функционирования, стабильности объектов путем предотвращения и снижения возможного ущерба от деструктивных информационных воздействий на защищаемые объекты КИИ;
- Блокирование и нейтрализация угроз безопасности информации, которые могут привести к нарушению штатного функционирования ОКИИ, контролируемых объектов и процессов;
- Локализация и минимизация последствий от возможной реализации угроз безопасности информации;
- Повышение уровня безопасности за счет внедрения современных средств защиты и диспетчеризации для событий ИБ, возникающих в ОКИИ.

Дальнейшее развитие

- Масштабирование и модернизация систем информационной безопасности, с учетом изменения категорий значимости объектов КИИ и требований регуляторов;
- Внедрение системы сбора, анализа и корреляции событий ИБ, с целью выявления и расследования инцидентов (SIEM система);
- Внедрение системы обнаружения вторжений для промышленных сетей с целью анализа трафика промышленных сетей для выявления отклонений в значениях технологических параметров, обнаружения признаков сетевых атак и контроля работы и текущего состояния устройств в сети (IDS система).

СПАСИБО
ЗА ВНИМАНИЕ!