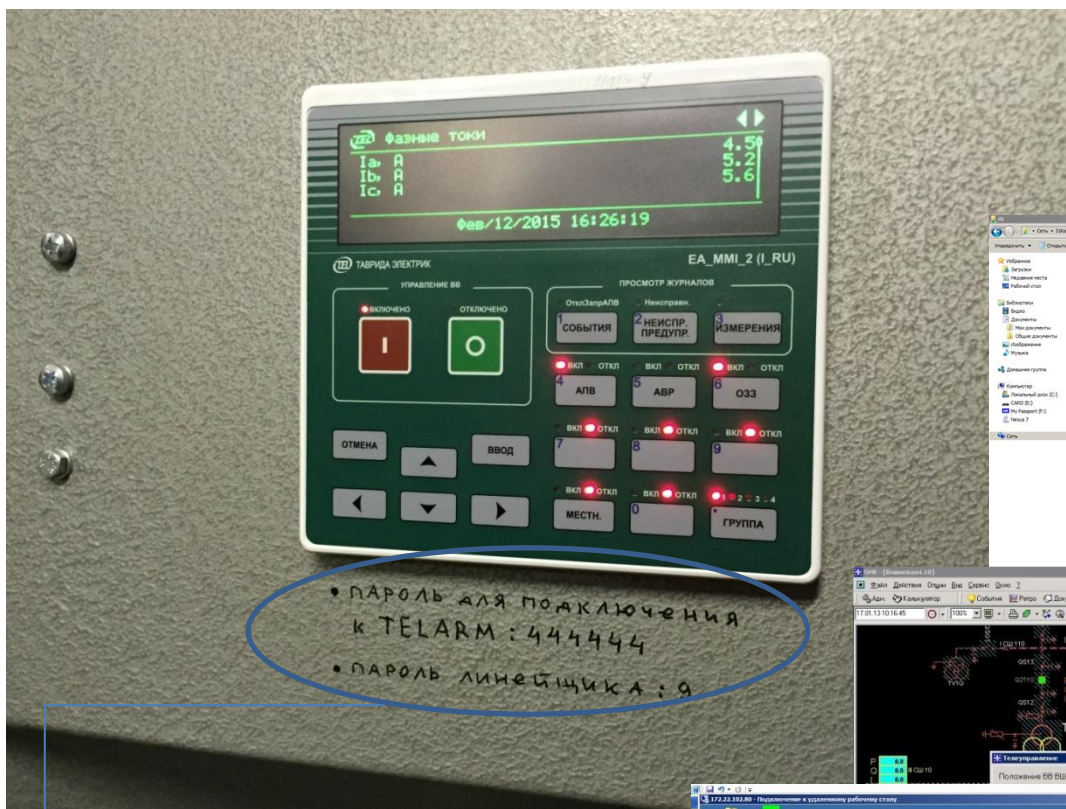




Подходы к обеспечению информационной безопасности объектов электросетевого комплекса

Начальник отдела информационной безопасности
Департамента безопасности
Зайцев Алексей Андреевич

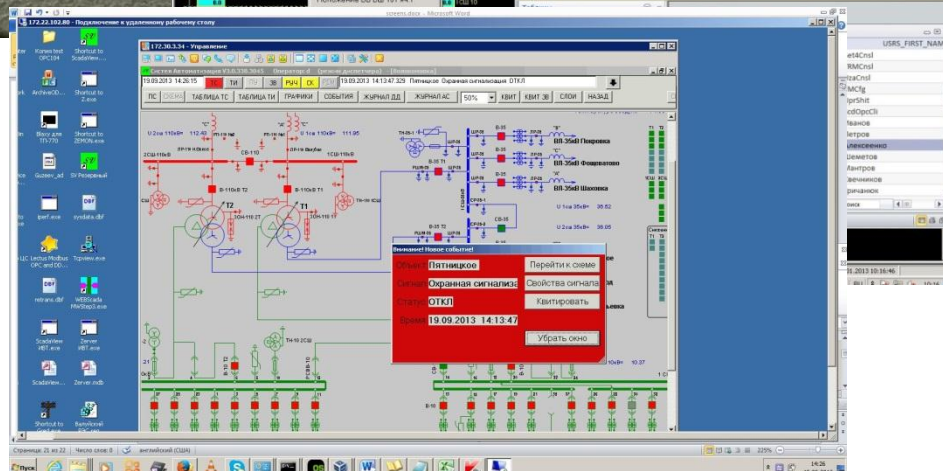
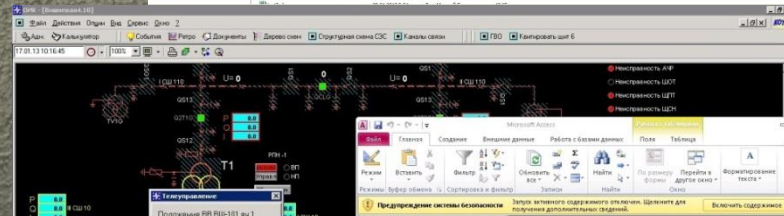
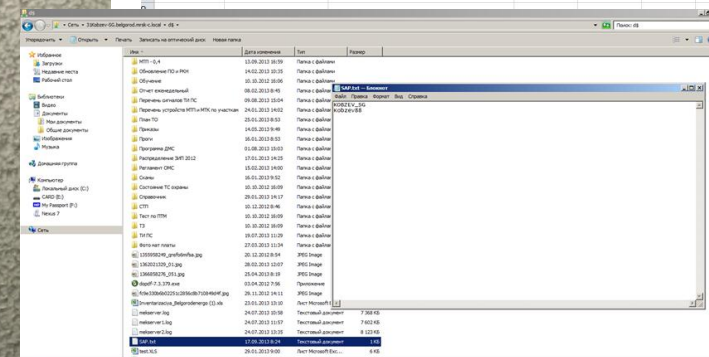
июнь 2015



• ПАРОЛЬ ДЛЯ ПОДКЛЮЧЕНИЯ
к TELARM: 444444
• ПАРОЛЬ ЛИНЕЙЩИКА: 9

Приклеенные пароли на
мониторах рабочих станциях,
сохраненные в файлах и
написанные на технологическом
оборудовании!

Буфер обмена		Шрифт	Выравнивание	Число
A1	Вишневая			
A	Вишневая			
1	Видеорегистратор Acipmen 1	логин	пароль	
2	10.168.8.2-50000	USER	123	
3	10.168.8.3-50000	USER	123	
4	10.168.8.11	root	123456	
5	10.168.8.12	root	123456	





- система мониторинга безопасности не видит событий из 80% информационных систем
- маршруты или правила написаны в обход межсетевого экрана
- антивирусная система отключена
- база системы предотвращения утечек забита на 80% и давно не регистрирует инциденты
- системы обнаружения вторжений генерируют более 10 миллиона событий в день
- сотрудник безопасности не может и не знает что делать в случае инцидента
- вокруг средств и систем безопасности выстраивается другая инфраструктура



- Отсутствие детальных стандартов и лучших практик по настройке систем безопасности, информационных и технологических систем.
- Стандарты в области ИБ носят высокоуровневый характер
- Подрядчики в области ИБ - это в первую очередь компании заинтересованные в получении прибыли, даже если они проявляют альтруизм - специфика работы у заказчиков им неизвестна, в результате получается продажа и внедрение коробок, а не процессов обеспечения ИБ.



Не умеешь? – НАУЧИМ!

Не хочешь? – ЗАСТАВИМ!

Остальные сами разбегутся ...

- Разработка стандартов и систем оценок и сертификации реально позволяющих оценить эффективность информационной безопасности
- Разработка метрик эффективности
- Разработка требований к типовой численности персонала, способной обеспечивать безопасность заданного числа объектов
- Разработка типовых технических решений в виде стандартов организаций или отраслевых стандартов
- Стандартизировать настройки и условия эксплуатации систем информационной безопасности



**Хорошего специалиста
информационной
безопасности – можно
уволить только по причине
его качественной работы.**

Спасибо за внимание!

