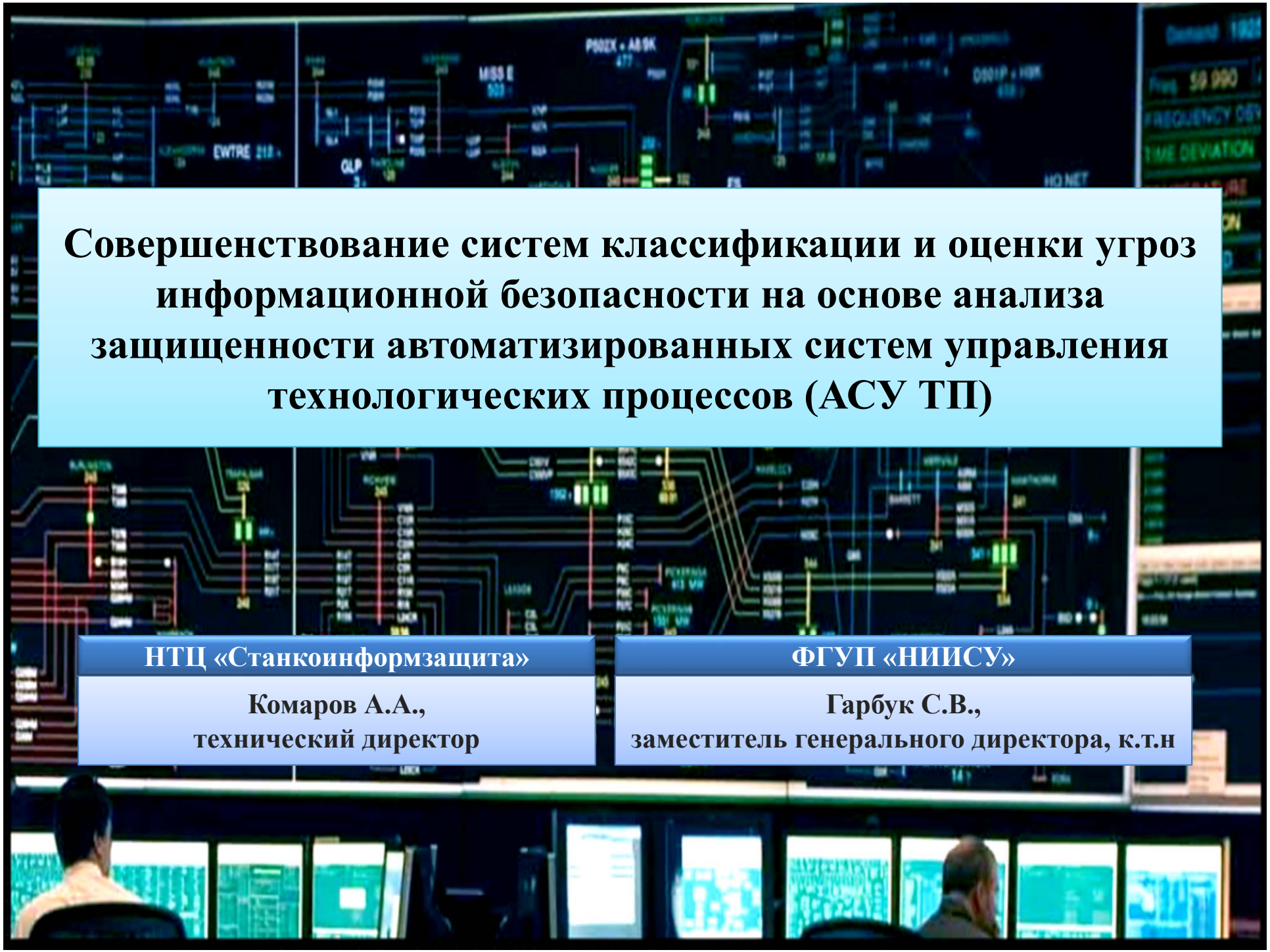


Совершенствование систем классификации и оценки угроз информационной безопасности на основе анализа защищенности автоматизированных систем управления технологических процессов (АСУ ТП)

НТЦ «Станкоинформзащита»	ФГУП «НИИСУ»
Комаров А.А., технический директор	Гарбук С.В., заместитель генерального директора, к.т.н

Факты и тенденции

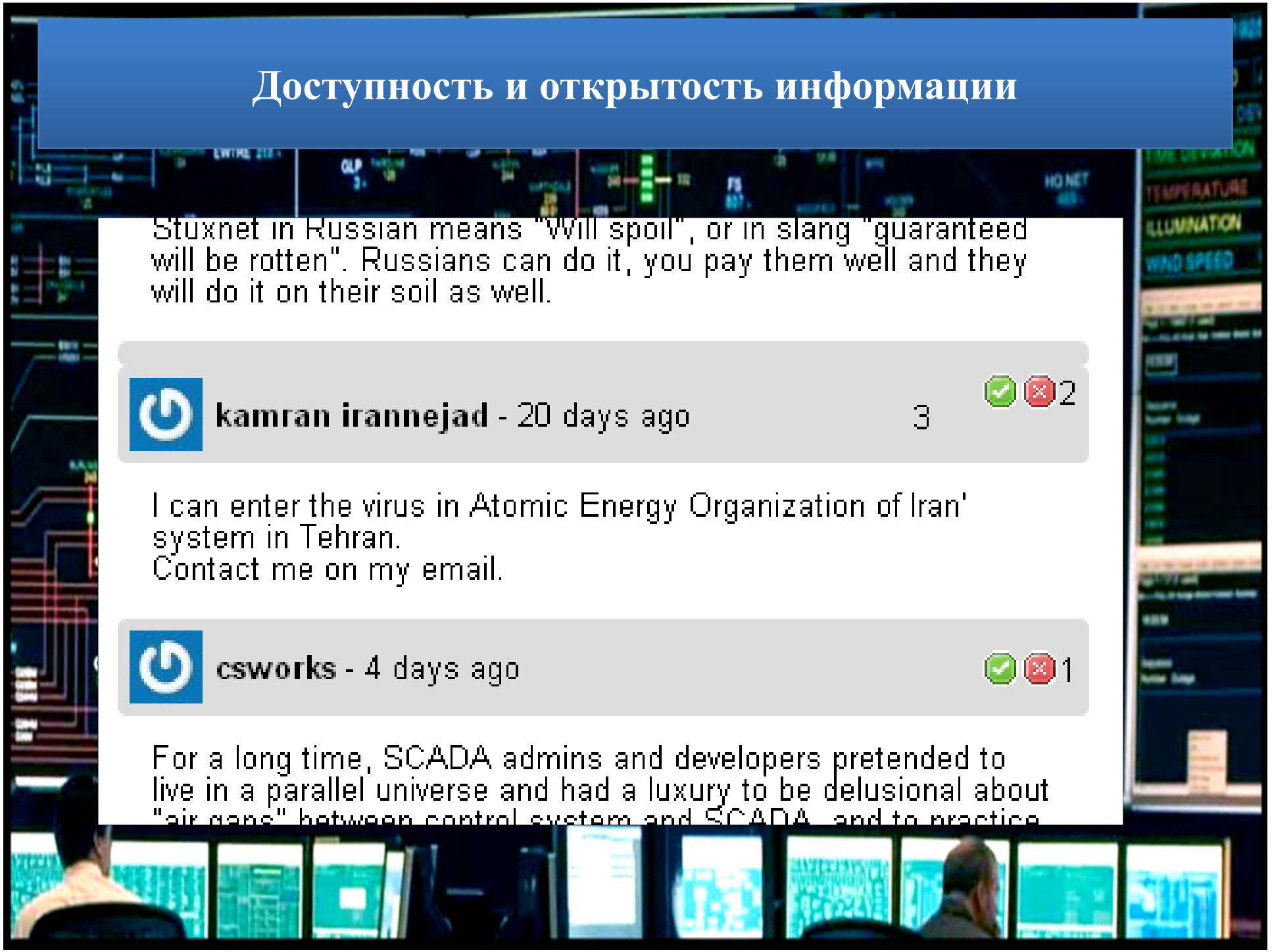
За период 2010-2011 гг. обнаружено более 50 новых уязвимостей в программном обеспечении АСУ ТП зарубежных государств

Обнаружен первый специализированный экземпляр вредоносного кода под платформу SCADA («Stuxnet»), организующий изменения в логике программируемых логических контроллеров (PLC)

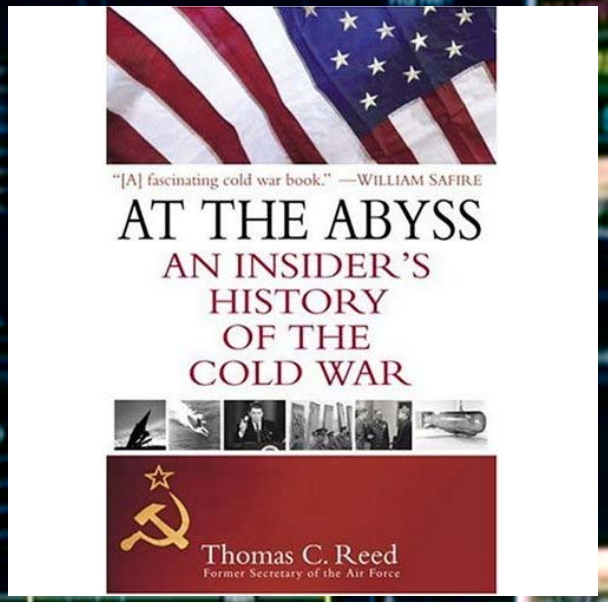
На рынке средств защиты информации появились профильные средства защиты информации АСУ ТП (СК-Proxy («Монитор-электрик»), SCADA-Аудитор 1.2. (НТЦ «Станкоинформзащита»), Tofino Industrial Firewall LSM (Tofino Security)).

Российские компании «стали» заниматься аудитом защищенности ИБ АСУ ТП в качестве одной из флагманских услуг

Доступность и открытость информации



Сокрытие информации о надежности и импортозамещение



«How the CIA Hacked a Russian SCADA Network»

"The pipeline software that was to run the pumps, turbines, and values was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds."

Успешные примеры проектов по стандартизации и классификации отдельных узкоспециализированных вопросов информационной безопасности

WEB-приложения

Web Application Threat Classification (WATC, WASC)

VoIP

VoIP Security Threat Taxonomy (VSTT, VoIPSA)

Беспроводные сети (3G)

A Taxonomy of Cyber Attacks on 3G Networks (The Pennsylvania State University)

Вредоносный и злонамеренный код

Malware Attribute Enumeration and Characterization (MAEC, Mitre)

Gramma Tech,
Klockwork,
Cigital Gary McGraw,
Secure Software CLASP,
Fortify,
Ounce Labs

Цели, задачи и исходные данные для классификации

Что возможно?

Единая классификация угроз ИБ АСУ ТП

С помощью чего?

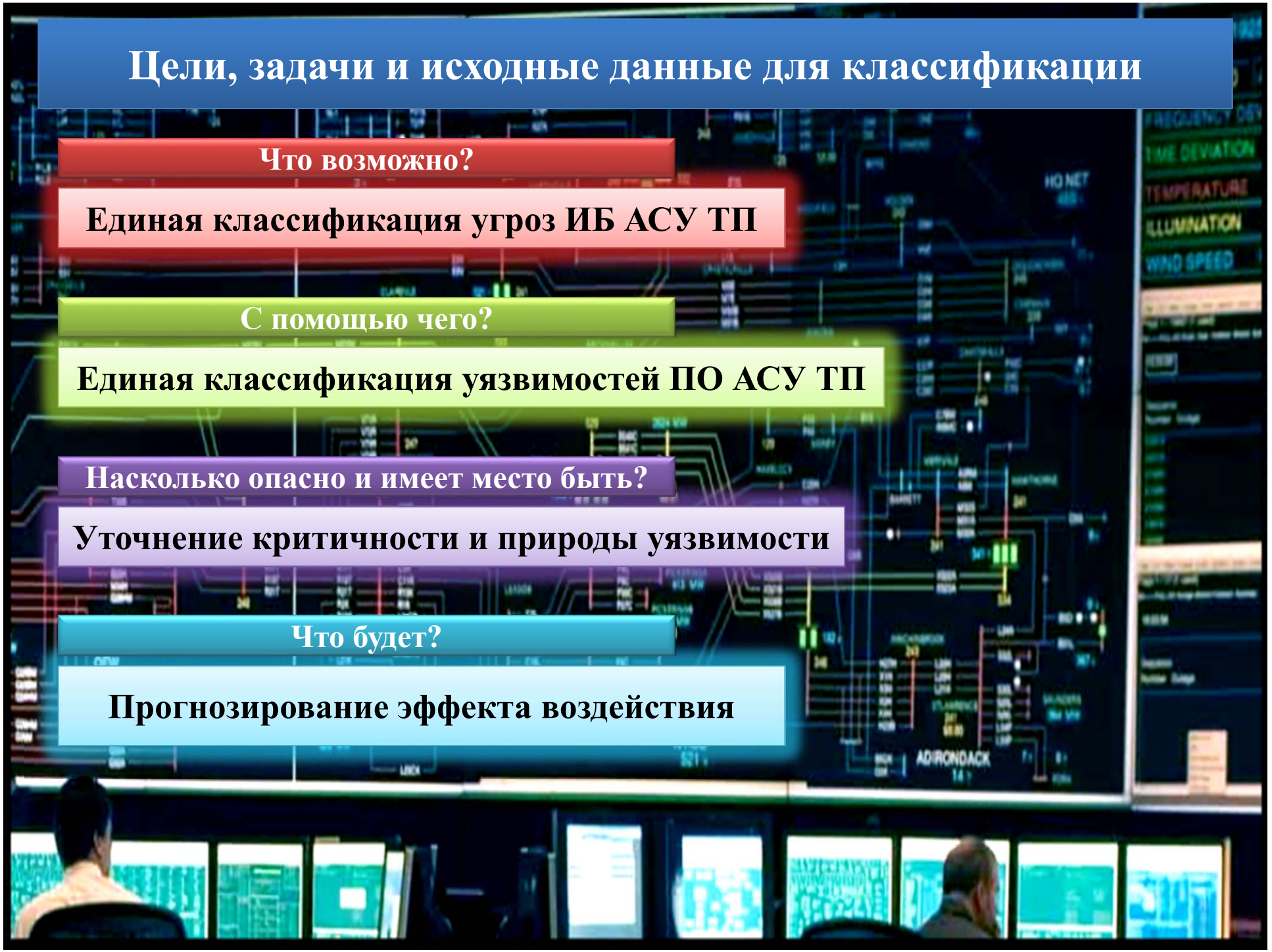
Единая классификация уязвимостей ПО АСУ ТП

Насколько опасно и имеет место быть?

Уточнение критичности и природы уязвимости

Что будет?

Прогнозирование эффекта воздействия



Исходные данные и их источники

Уязвимости, обнаруженные НТЦ «Станкоинформзащита»

[STANKOINFORMZASCHITA-10-04] ICSCADA (Outlaw Automation)
[STANKOINFORMZASCHITA-10-03] Broadwin SCADA
[STANKOINFORMZASCHITA-10-02] ITS SCADA
[STANKOINFORMZASCHITA-10-01] Netbiter® webSCADA …

Нормативно-регламентная и рекомендательная база зарубежных государств

- NERC CIP, FERC CIP, AGA 12 …
- архивы баз знаний учёта выявленных инцидентов производителя
- архивы баз знаний профильных групп и сообществ

Учёт и анализ инцидентов ИБ АСУ ТП зарубежных государств

- база инцидентов ИБ «RISI»
- архив базы знаний US CERT / «Control Systems»
- международные профильные СМИ

Единая классификация угроз ИБ АСУ ТП

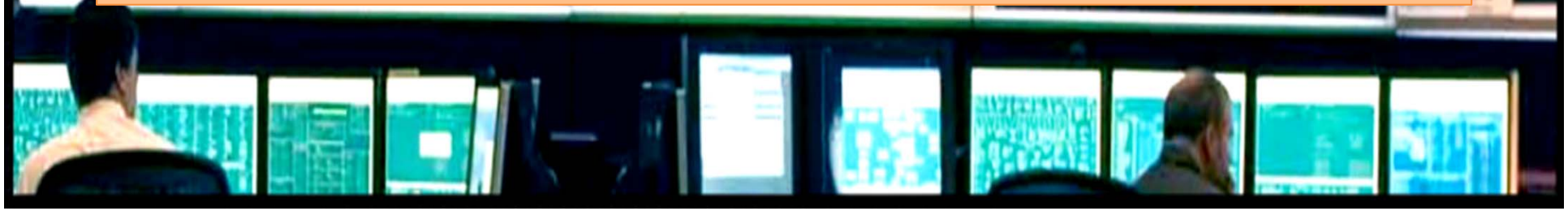
«Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007)

«Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007)

Гармонизация с классификацией CAPEC
(Common Attack Pattern Enumeration and Classification)

Гармонизация с классификацией CWE / SAN
(CWE-751:Top 25 - Insecure Interaction Between Components)

Дополнение и уточнение механизмов специфичных атак
(CAPEC-1000: Mechanism of Attack)



Разделы системы классификации

Протокол ICCP (TASE.2).

1. Неавторизированный доступ к ICCP-серверу.
Эксплуатация уязвимостей в ПО ICCP-сервера или платформе его управления, получение управления над ICCP-сервером.

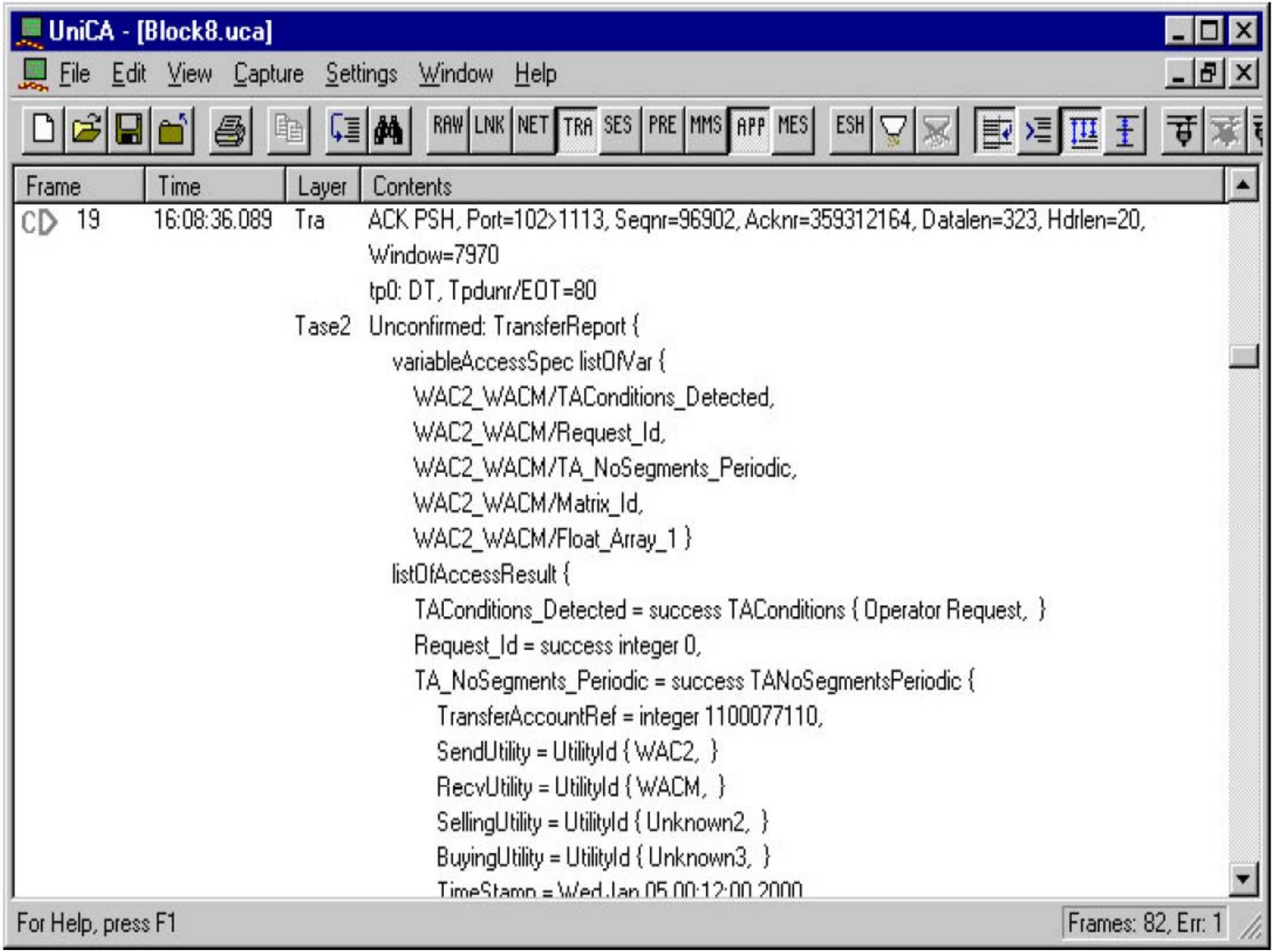
2. Неавторизированный запрос ассоциации клиента к ICCP-серверу.
Позволяет опознать ICCP-сервер и уточнить его сетевые характеристики в качестве одного из способа проведения активной сетевой компьютерной разведки.

3. Множественные запросы ассоциации к ICCP-серверу с использованием протокола транспортного уровня модели OSI с установкой логического соединения (OSI Connection Oriented Transport Protocol).

4. **Неавторизированный запрос на запись переменной MMS** (спецификация производственных сообщений, ISO 9506) в отношении окружения ICCP-сервера.

6. **Неавторизированный доступ путём эксплуатации брешей конфигурации ICCP-сервера в отношении коммуникации с использованием сторонних протоколов передачи данных.** (LiveData ICCP Server ISO Transport Service Over TCP Buffer Overflow Vulnerability , ISO transport service)

7. **Дешифровка и анализ содержимого ICCP/MMS-пакетов** (могут быть использованы специализированные пакетные анализаторы класса «Kema UniCA analyzer»).


UniCA - [Block8.uca]
File Edit View Capture Settings Window Help
RAW LNK NET TRA SES PRE MMS APP MES ESH
Frame Time Layer Contents
19 16:08:36.089 Tra ACK PSH, Port=102>1113, Seqnr=96902, Acknr=359312164, Datalen=323, Hdrlen=20,
Window=7970
tp0: DT, Tpdunr/EOT=80
Tase2 Unconfirmed: TransferReport {
variableAccessSpec listOfVar {
WAC2_WACM/TAConditions_Detected,
WAC2_WACM/Request_Id,
WAC2_WACM/TA_NoSegments_Periodic,
WAC2_WACM/Matrix_Id,
WAC2_WACM/Float_Array_1 }
listOfAccessResult {
TAConditions_Detected = success TAConditions { Operator Request, }
Request_Id = success integer 0,
TA_NoSegments_Periodic = success TANoSegmentsPeriodic {
TransferAccountRef = integer 1100077110,
SendUtility = UtilityId { WAC2, }
RecvUtility = UtilityId { WACM, }
SellingUtility = UtilityId { Unknown2, }
BuyingUtility = UtilityId { Unknown3, }
TimeStamp = Wed Jan 05 00:12:00 2000
For Help, press F1
Frames: 82, Err: 1

Разделы системы классификации

Протокол DNP3

1. Выявление устройств программируемых логических контроллеров (PLC) и DNP3-серверов путём рассылки широковещательных запросов в сегменте технологической сети.
(DNP3 поддерживает оповещение всех устройств для их выявления путём рассылки широковещательного запроса на адрес вида «FFFF»).

2. **Выявление устройств программируемых логических контроллеров (PLC) и DNP3-серверов путём организации «point list»-сканирования.**
Уточнение доступных слотов DNP3-сервера и определение их свойств.

3. **Выявление устройств программируемых логических контроллеров (PLC) и DNP3-серверов путём организации «function list»-сканирования.**
Уточнение доступных DNP3-серверов по характерным кодам ошибок.

4. **Проведение атак класса «Человек по середине» в виду отсутствия процедур аутентификации в протоколе.**
Организационно-технические меры и контроль подключенных клиентов сети.

5. **Извлечение значений контрольных сумм и уточнение алгоритмов её генерации при использовании реализации «DNP3 over TCP» для негласного внедрения в эфир.**

Разделы системы классификации

Протокол DNP3

6. Останов приложений DNP3-сервера путём посылки специально сформированного пакета с функциональным кодом 12 и указанием имени приложения.

7. Блокировка получения DNP3-сервером сообщений об ошибках и возможных сигналах аварийных ситуаций от программируемых логических контроллеров (PLC) путём рассылки им пакета с функциональным кодом 15 «Disable Unsolicited».

8. Нарушение корректной работы DNP-3 сервера путем отправки модифицированного пакета с функциональным кодом «0D», переводящим устройства в режим перезагрузки («Cold Restart function code»).

9. Сброс событий DNP-3 сервера и перезагрузка его конфигурации путём отправки модифицированного пакета с функциональным кодом «0E» («Warm Restart function code»).

10. Неавторизированная модификация временных характеристик полевых устройств и устройств программируемых логических контроллеров путём посылки специально сформированного пакета с функциональным кодом 2 (object type 50).

Разделы системы классификации

Протокол MODBUS

1. Неавторизированный запрос на чтение текущего состояния группы логических ячеек.
(«READ COIL STATUS»)

2. Неавторизированный запрос на чтение текущего состояния группы дискретных входов.
(«READ INPUT STATUS»)

3. Неавторизированный запрос на чтение значения одного или нескольких регистров хранения.
(«READ HOLDING REGISTERS»)

4. Неавторизированный запрос на чтение значения одного или нескольких входных регистров.
(«READ INPUT REGISTERS»)

5. Неавторизированный запрос на изменение логической ячейки в другое состояние.
(«FORCE SINGLE COIL»)

Разделы системы классификации

Протокол MODBUS

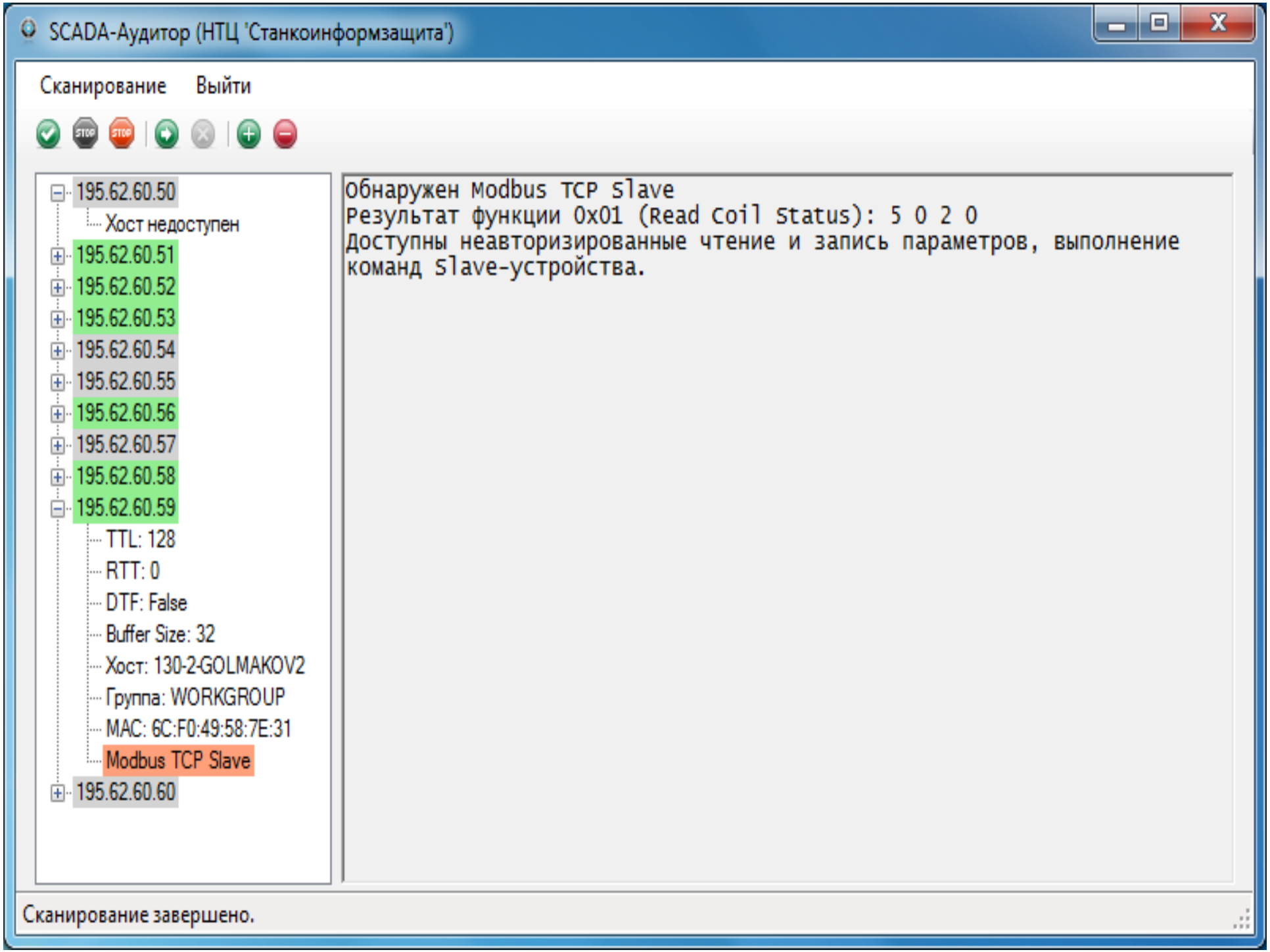
6. Неавторизированный запрос на запись нового значения в регистр хранения.
(«FORCE SINGLE REGISTER»)

7. Неавторизированное получение состояния восьми внутренних логических ячеек, чье назначение зависит от типа контроллера.
(«READ EXCEPTION STATUS»)

8. Неавторизированное изменение нескольких последовательных регистров.
(«FORCE MULTIPLE REGISTERS»)

9. Неавторизированное чтение типа адресуемого «Slave» и определение его рабочего состояния.
(«REPORT SLAVE I.D»)

10. Неавторизированный перевод сервера Modbus в режим «listen only».
(разрывает связь со всеми ПЛК)


SCADA-Аудитор (НТЦ 'Станкоинформзащита')
Сканирование
Выйти
195.62.60.50
Хост недоступен
195.62.60.51
195.62.60.52
195.62.60.53
195.62.60.54
195.62.60.55
195.62.60.56
195.62.60.57
195.62.60.58
195.62.60.59
TTL: 128
RTT: 0
DTF: False
Buffer Size: 32
Хост: 130-2-GOLMAKOV2
Группа: WORKGROUP
MAC: 6C:F0:49:58:7E:31
Modbus TCP Slave
195.62.60.60
Обнаружен Modbus TCP Slave
Результат функции 0x01 (Read Coil Status): 5 0 2 0
Доступны неавторизированные чтение и запись параметров, выполнение команд Slave-устройства.
Сканирование завершено.

Единая классификация уязвимостей ПО АСУ ТП

«TOP 10 VULNERABILITIES OF CONTROL SYSTEMS AND THEIR ASSOCIATED MITIGATIONS – 2006» (NERC / NSTB)

Привязка к промышленным сетевым протоколам с учётом брешей их реализации и функциональных особенностей

Привязка к специальным службам и сервисам АСУ ТП (OPC, OPC-bridge, OPC-relay, Historian, DDE)

Уточнение критичности и природы уязвимости

Использование CVSS (Common Vulnerability Scoring System)

Использование CWSS (Common Weakness Scoring System)

Уточнение описания «General Modifiers»
Organization specific potential for loss(CollateralDamagePotential)

High (catastrophic loss) **– когда*?**
(признаки, условия)

Прогнозирование эффекта воздействия

«Cyberwarfare and its damaging effects on citizens» (by Stefano Mele)

Инструкция по расследованию и учету технологических нарушений в работе энергосистем, электростанций, котельных, электрических и тепловых сетей (СО 153-34.20.801-00)

К аварийным ситуациям в энергосистемах относят:

- работу энергосистемы или её части с частотой 49,2 Гц и ниже в течение одного часа и более продолжительностью в течение суток более трёх часов;

- аварийное отключение потребителей суммарной мощностью более 500 МВт или 50 % от общего потребления энергосистемой вследствие отключения генерирующих источников, линий электропередачи разделения энергосистемы на части;

-нарушение режима работы электрической сети, вызвавшее перерыв электроснабжения города на 24 часа и более.

Прогнозирование эффекта воздействия
Пример 1.

Угроза: нарушение физической безопасности периметра КВО

Подавление организационно-технических мер, необходимых для обеспечения физической безопасности и сохранности элементов КВО

Атака: отключение системы контроля участка транспортировки углеводородов

Отключение системы оповещения о несанкционированном приближении объекта в непосредственную близость участка КВО класса «RadioBarier»

Уязвимость: Раскрытие информации в АСУ оповещения и сигнализирования тревог

Отключение системы оповещения о несанкционированном приближении стороннего объекта (Remote Alarm Management System (RAMS)) в участок непосредственной близости с границами КВО

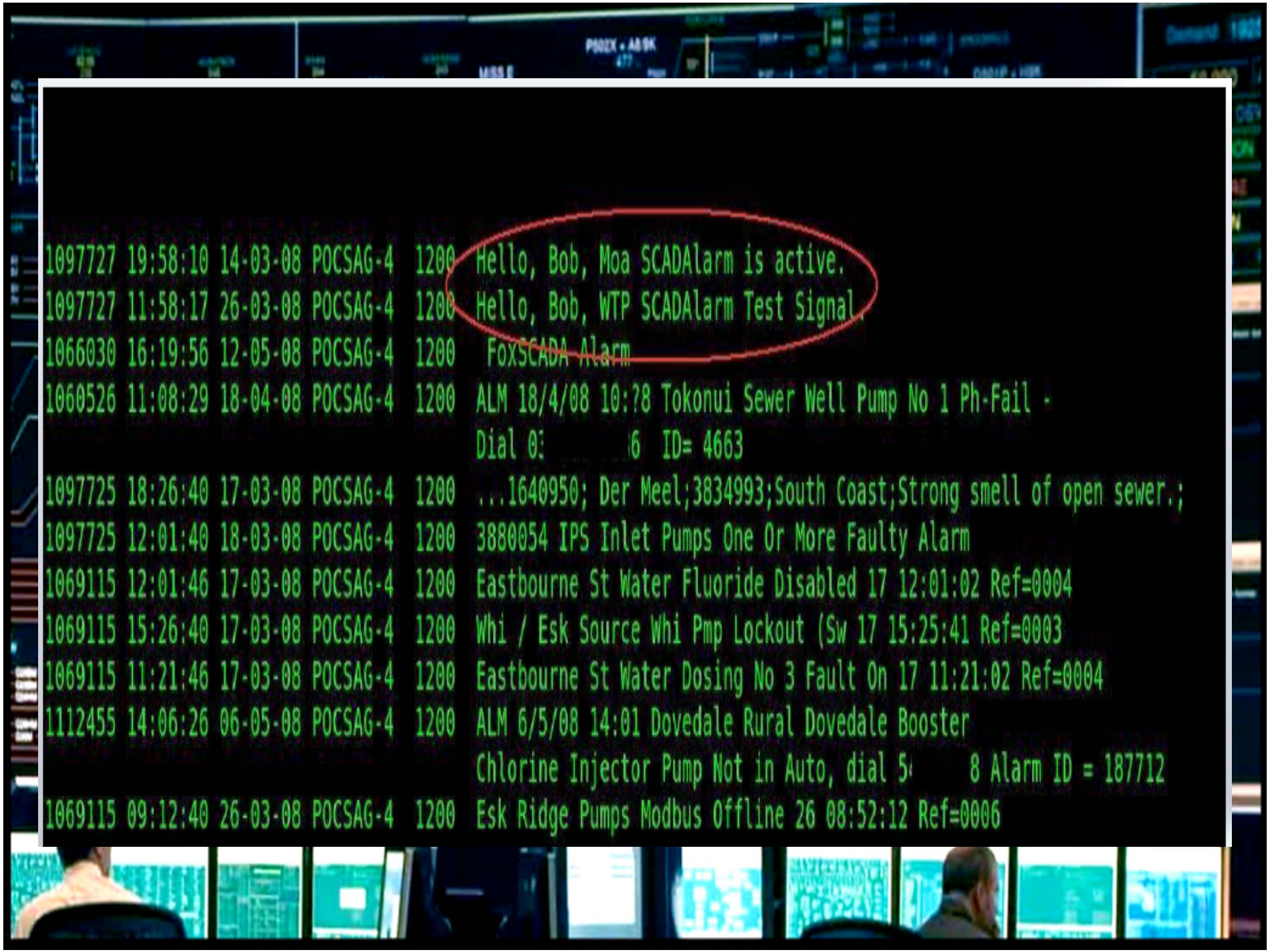
Эффект от информационного воздействия

Проникновение в зону непосредственной близости КВО

Alarm Proxy Service – TCP 4122
Data Service – TCP 4124
Camera Service – TCP 4123
Relay Service – TCP 4128
WMI Service для отправки уведомлений

Платформа: ОС Windows XP SP 2
Уязвимость: нулевая сессия

Использование возможностей WMI-транспорта


1097727 19:58:10 14-03-08 POCSAG-4 1200 Hello, Bob, Moa SCADAlarm is active.
1097727 11:58:17 26-03-08 POCSAG-4 1200 Hello, Bob, WTP SCADAlarm Test Signal
1066030 16:19:56 12-05-08 POCSAG-4 1200 FoxSCADA Alarm
1060526 11:08:29 18-04-08 POCSAG-4 1200 ALM 18/4/08 10:?8 Tokonui Sewer Well Pump No 1 Ph-Fail -
Dial 0: 6 ID= 4663
1097725 18:26:40 17-03-08 POCSAG-4 1200 ...1640950; Der Meel;3834993;South Coast;Strong smell of open sewer.;
1097725 12:01:40 18-03-08 POCSAG-4 1200 3880054 IPS Inlet Pumps One Or More Faulty Alarm
1069115 12:01:46 17-03-08 POCSAG-4 1200 Eastbourne St Water Fluoride Disabled 17 12:01:02 Ref=0004
1069115 15:26:40 17-03-08 POCSAG-4 1200 Whi / Esk Source Whi Pmp Lockout (Sw 17 15:25:41 Ref=0003
1069115 11:21:46 17-03-08 POCSAG-4 1200 Eastbourne St Water Dosing No 3 Fault On 17 11:21:02 Ref=0004
1112455 14:06:26 06-05-08 POCSAG-4 1200 ALM 6/5/08 14:01 Dovedale Rural Dovedale Booster
Chlorine Injector Pump Not in Auto, dial 5 8 Alarm ID = 187712
1069115 09:12:40 26-03-08 POCSAG-4 1200 Esk Ridge Pumps Modbus Offline 26 08:52:12 Ref=0006

Прогнозирование эффекта воздействия
Пример 1.

Прогнозирование эффекта воздействия
Пример 2.

Угроза: Нарушение корректного исполнения технологического процесса

Подавление организационно-технических мер, необходимых для автоматизации технологического процесса

Атака: НСД к системе диспетчеризации

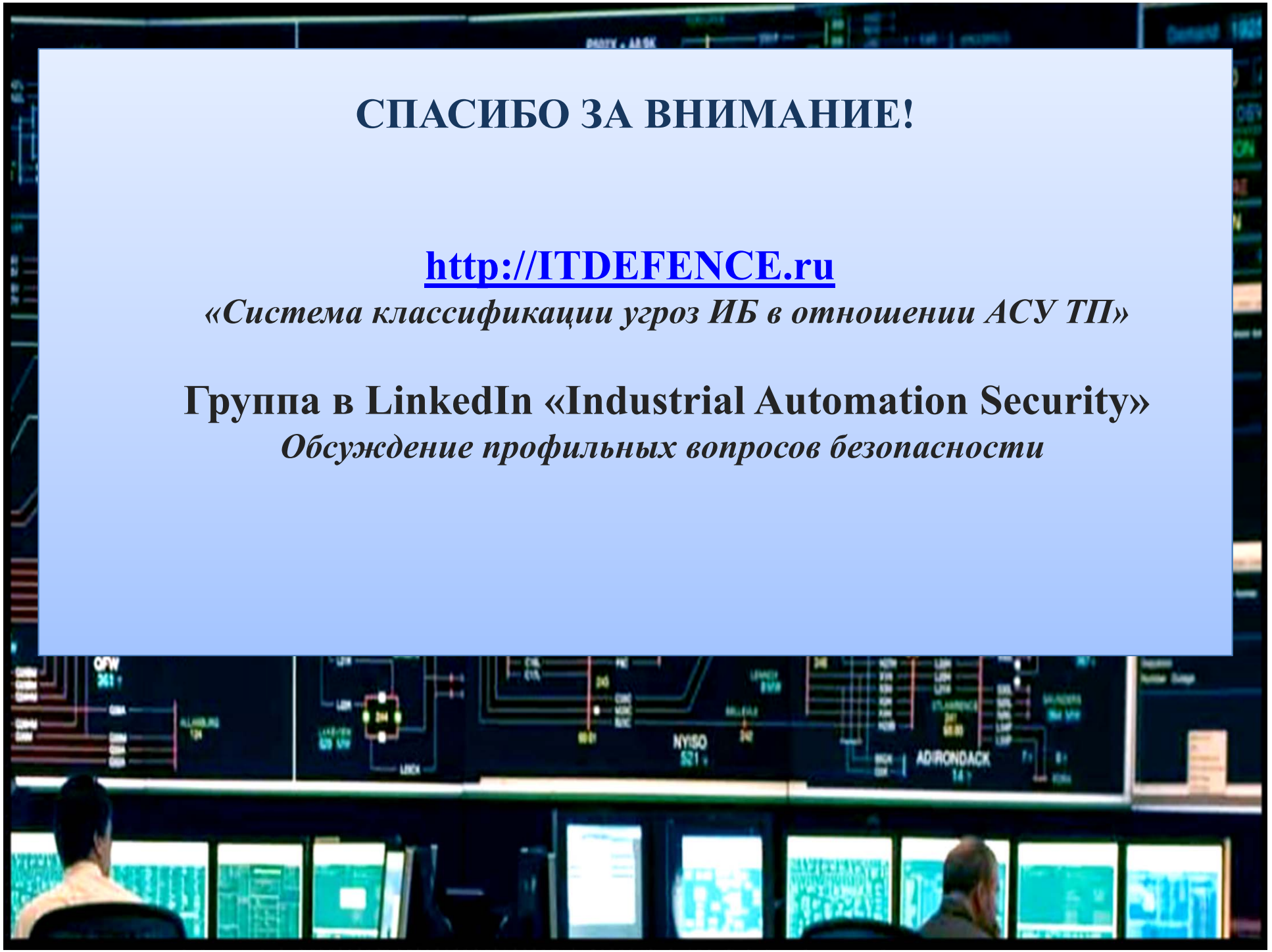
Получение привилегированного доступа к системе SCADA

Уязвимость: Переполнение буфера компонента Citect SCADA

Эксплуатация компонентов ODBC

Эффект от информационного воздействия: отсутствует

Наличие модулей ПАЗ



СПАСИБО ЗА ВНИМАНИЕ!

http://ITDEFENCE.ru

«Система классификации угроз ИБ в отношении АСУ ТП»

Группа в LinkedIn «Industrial Automation Security»

Обсуждение профильных вопросов безопасности