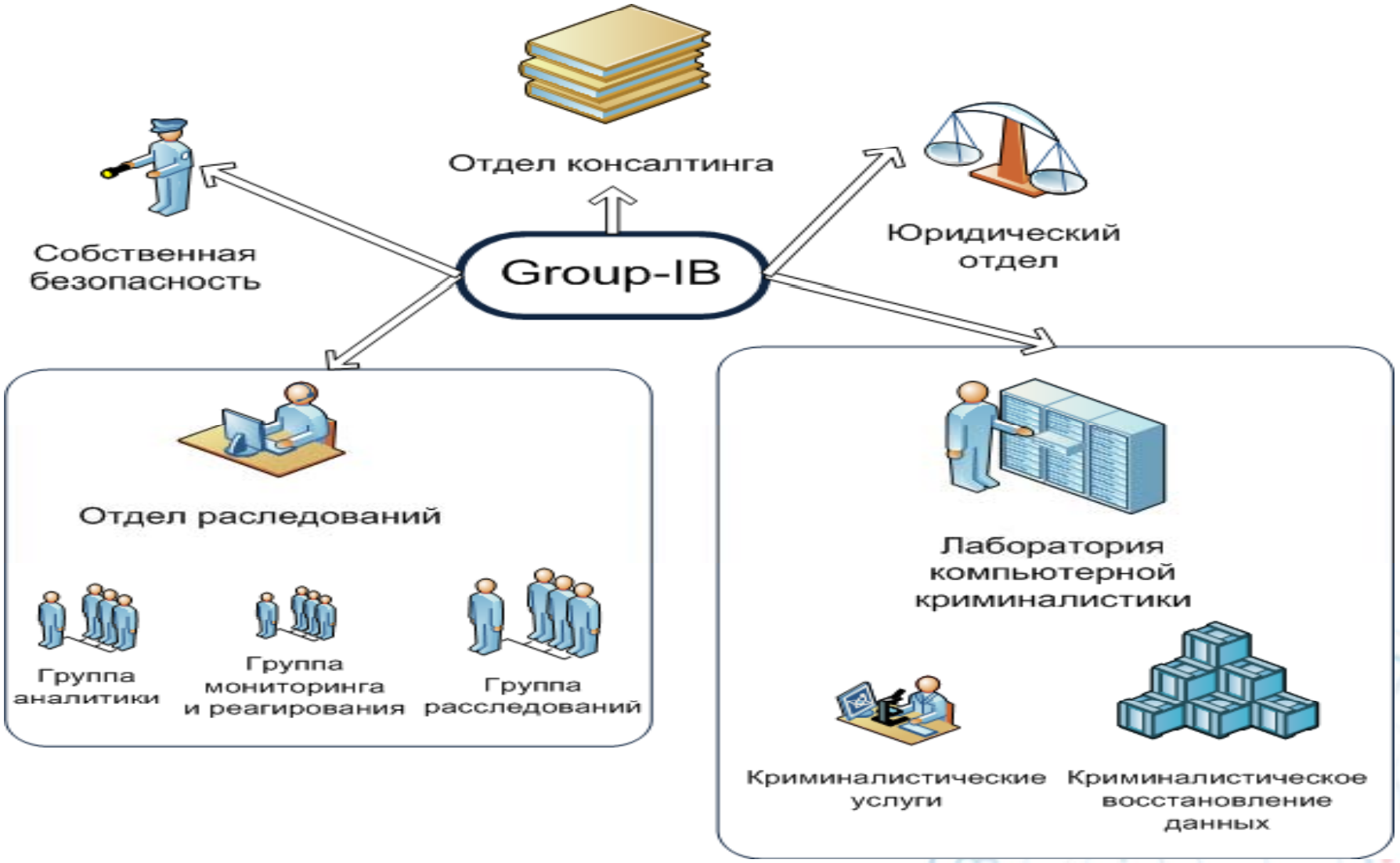
Средства защиты информации в АСУ ТП: текущее состояние и перспективы развития

Group-IB

- ✓ **Первая и единственная негосударственная компания в РФ, оказывающая комплексные услуги консалтинга в области расследования инцидентов информационной безопасности**
- ✓ **Основана в 2003**
- ✓ **Сотрудничество с экспертными организациями в 52 странах**
- ✓ **24/7мониторинг и поддержка**


Отдел консалтинга
Собственная безопасность
Group-IB
Юридический отдел
Отдел раследований
Группа аналитики
Группа мониторинга и реагирования
Группа расследований
Лаборатория компьютерной криминалистики
Криминалистические услуги
Криминалистическое восстановление данных

- ✓ Группы по реагированию на инциденты (CERT) в 52 странах мира
- ✓ Антивирусные компании
- ✓ Производители решений по компьютерной криминалистике и информационной безопасности
- ✓ Университеты США и Европы
- ✓ Международные организации по компьютерной криминалистике
- ✓ Ассоциация сертифицированных специалистов по борьбе с мошенничествами (ACFE)
- ✓ Центры изучения угроз информационной безопасности

Благодарность

Генеральному директору
ООО «Группа информационной безопасности»

И.К. Сачкову

Управление по борьбе с экономическими преступлениями ГУВД по г. Москве выражает благодарность коллективу ООО «Группа информационной безопасности» за оказываемое содействие в выявлении и пресечении преступлений, совершаемых с использованием сети Интернет.

Начальник УБЭП
ГУВД по г. Москве А.М. Данилов

приказ № 14686 от 13.09.2010г.

БСТМ
ГУ МВД России по г. Москве

Генеральному директору
ООО «Группа информационной безопасности»
И.К. Сачкову

Уважаемый Илья Константинович!

Главное Управление МВД России по г. Москве выражает благодарность коллективу ООО "Группа информационной безопасности" за оказание содействия сотрудникам БСТМ ГУ МВД России по г. Москве в проведении оперативно-следственных мероприятий, а также за качественное проведение экспертиз по уголовному делу № 379968, ч. 4, ст. 159 УК РФ, способствовавших задержанию с поличным и изобличению в совершении преступлений организованной преступной группы.

Заместитель начальника К.Г. Кузнецов

Отдел "К"
УВД по Брянской области
выражает искреннюю благодарность

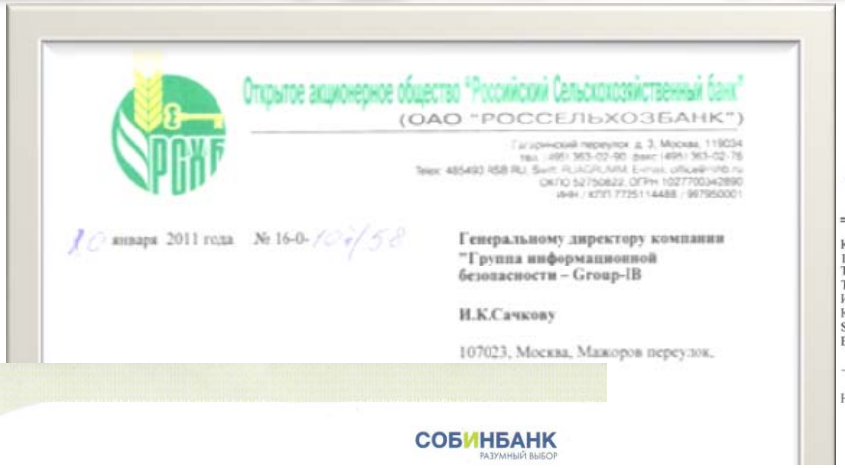
компании
Group IB
и лично
Илье Сачкову
Александру Писемскому
Дмитрию Волкову

Самой профессиональной команде в области расследования киберпреступлений.

Начальник отдела "К"
УВД по Брянской области Каршков С.С.

Брянск 2011г.

GROUP IB



Открытое акционерное общество "Российский Сельскохозяйственный банк"
(ОАО "РОССЕЛЬХОЗБАНК")

10 января 2011 года № 16-0-10-4/58

Генеральному директору компании
"Группа информационной
безопасности – Group-IB

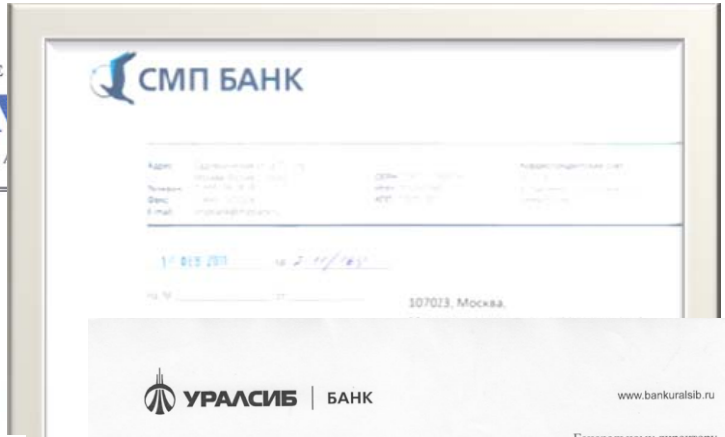
И.К.Сачкову

107023, Москва, Мажоров переулок,

КОММЕ
СДМ
ОТКРЫТОЕ А

КБ «СДМ-БАНК» (ОАО)
125424, Москва, Волоколамское шоссе, 73
Тел.: (495) 705-90-90, 490-15-45, факс: (495) 490-65-09
Телефакс: 911096 SDM-RU
ИНН 7733043350
Корр. сч. 30101810600000000685, БИК 044583685
SWIFT CODE SJSCRUMM
E-mail: post@sdm.ru, www.sdm.ru
27 ИЮЛ 2009 № 4493/110000

На № _____ от _____



СМП БАНК

107023, Москва,

СОБИНБАНК
РАЗУМНЫЙ ВЫБОР

28 ЯНВ 2011 No. 62-5-19/239117

Генеральному директору
Group-IB
г-ну Сачкову И.К.

Уважаемый Илья Константинович!

Коллектив Департамента безопасности ОАО «Собинбанк» выражает признательность за вклад Вашей компании Group-IB в дело обеспечения информационной безопасности ОАО «Собинбанк». Благодаря сотрудничеству с компанией Group-IB нам удалось предотвратить ряд инцидентов информационной безопасности, а так же провести расследования имевших место быть инцидентов.

Департамент безопасности ОАО «Собинбанк» надеется на дальнейшее успешное сотрудничество с компанией Group-IB в интересах обеспечения безопасности Банка, наших Клиентов и Партнеров.

Начальник Департамента безопасности
ОАО «Собинбанк»

А.Н. Косарев

27.01.2011

ОАО «СОБИНБАНК», 123022, Москва, ул. Рочдельская, д. 15, стр. 56. Тел.: (495) 725 2525, факс: (495) 725 2525. E-mail: mail@sobin.ru, www.sobinbank.ru

Swedbank

ОАО «Сведбанк»
125047, Москва, ул. Лесная, д. 5
Телефон, факс
+7 495 777 6363
+7 495 777 6364
www.swedbank.ru
Лицензия Банка России №3054
БИК 044579889 ОГРН 1027739131529
ИНН 7734051393 КПП 775001001

От _____ № _____
На № _____ от _____

Генеральному директору
ООО «Группа Информационной
безопасности»
САЧКОВУ И.К.

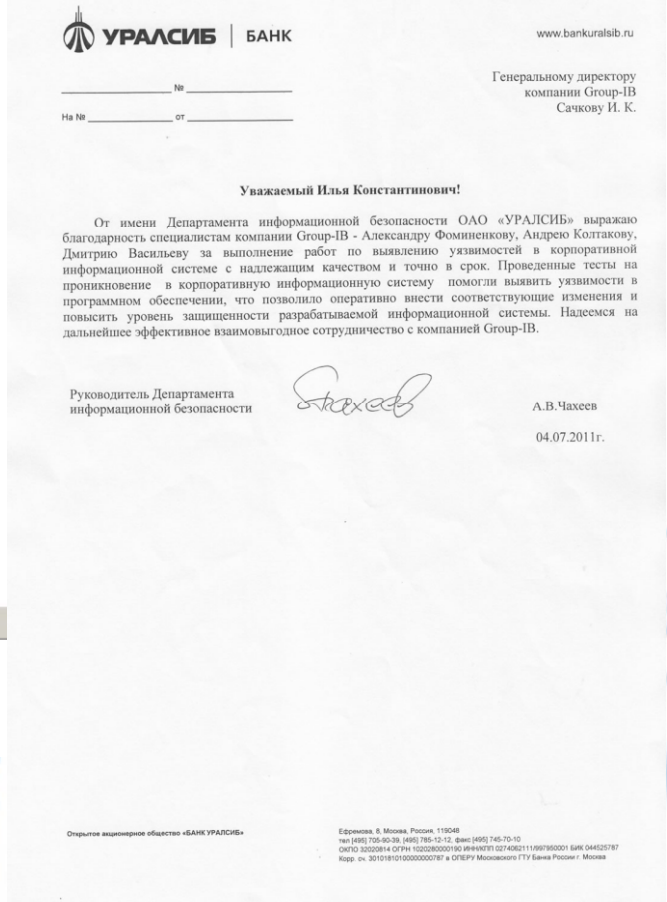
Уважаемый Илья Константинович!

От лица ОАО «Сведбанк» и от себя лично благодарю Вас и Вашу компанию за активное содействие в борьбе с киберпреступностью. Наш банк искренне желает Вам процветания, успеха в делах и финансового благополучия, и надеется на дальнейшее плодотворное сотрудничество.

Начальник Управления
риск-менеджмента,
член Правления

В.Г. Логофет

Исполнитель: Трубникова А.А.
Тел.777-6363 (доб. 1476)



УРАЛСИБ | БАНК

www.bankuralsib.ru

_____ № _____
На № _____ от _____

Генеральному директору
компании Group-IB
Сачкову И. К.

Уважаемый Илья Константинович!

От имени Департамента информационной безопасности ОАО «УРАЛСИБ» выражаю благодарность специалистам компании Group-IB - Александру Фоминенкову, Андрею Колтакову, Дмитрию Васильеву за выполнение работ по выявлению уязвимостей в корпоративной информационной системе с надлежащим качеством и точно в срок. Проведенные тесты на проникновение в корпоративную информационную систему помогли выявить уязвимости в программном обеспечении, что позволило оперативно внести соответствующие изменения и повысить уровень защищенности разрабатываемой информационной системы. Надеемся на дальнейшее эффективное взаимовыгодное сотрудничество с компанией Group-IB.

Руководитель Департамента
информационной безопасности

А.В.Чахеев

04.07.2011г.

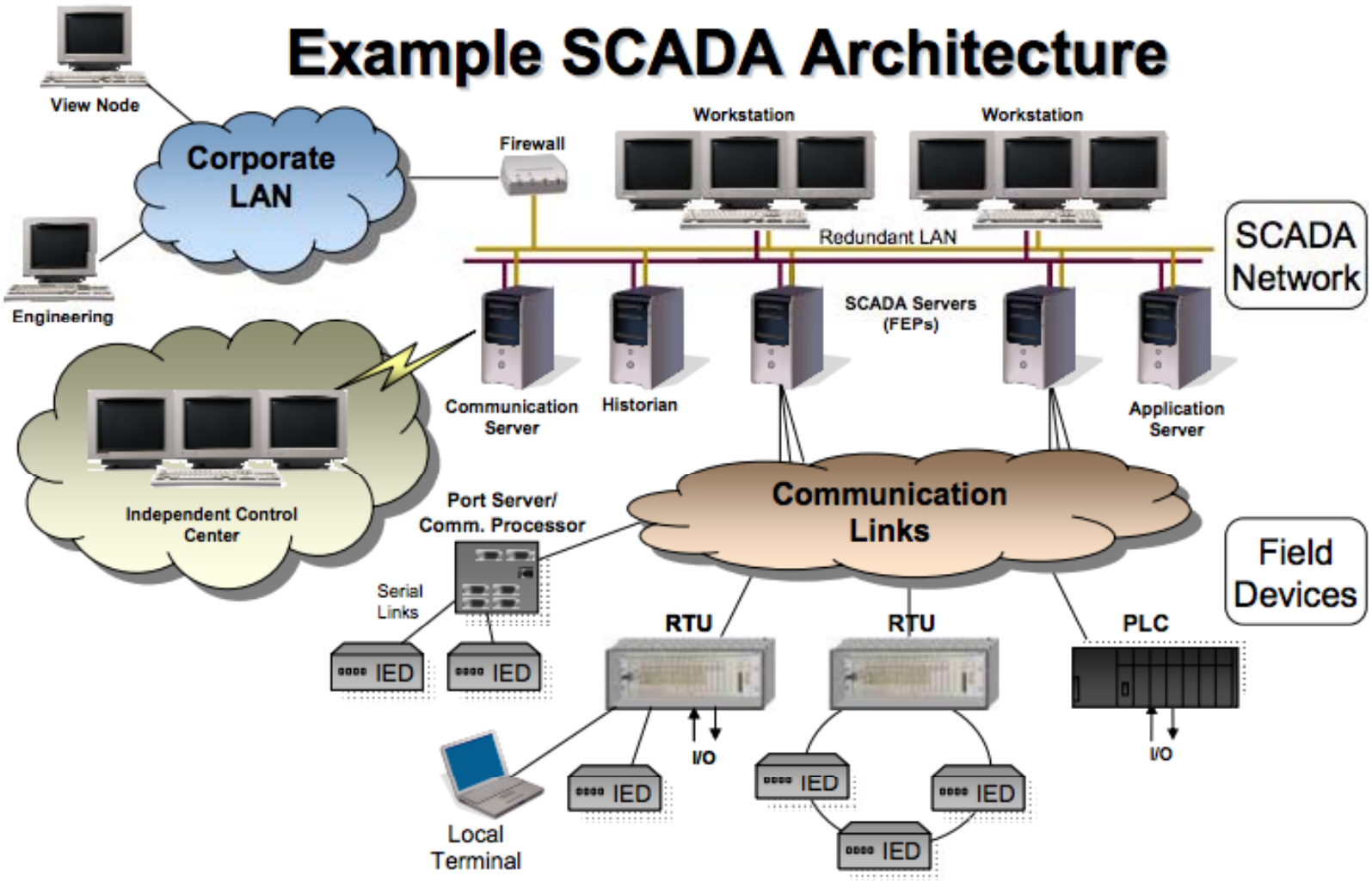
Открытое акционерное общество «БАНК УРАЛСИБ»

Ефремова, 8, Москва, Россия, 119048
тел.(495) 705-90-39, (495) 785-12-12, факс (495) 745-70-10
ОКПО 32020814 ОГРН 1020280000190 ИНН/КПП 0274062111/997950001 БИК 044525787
Корр. сч. 30101810100000000787 в ОПЕРУ Московского ГТУ Банка России г. Москва

АСУ ТП

- Автоматизированные системы управления технологическим процессом
- SCADA - Supervisory Control and Data Acquisition(Диспетчерское управление и сбор данных)
- ICS – Industrial Control Systems (Промышленные системы управления)

Пример архитектуры SCADA



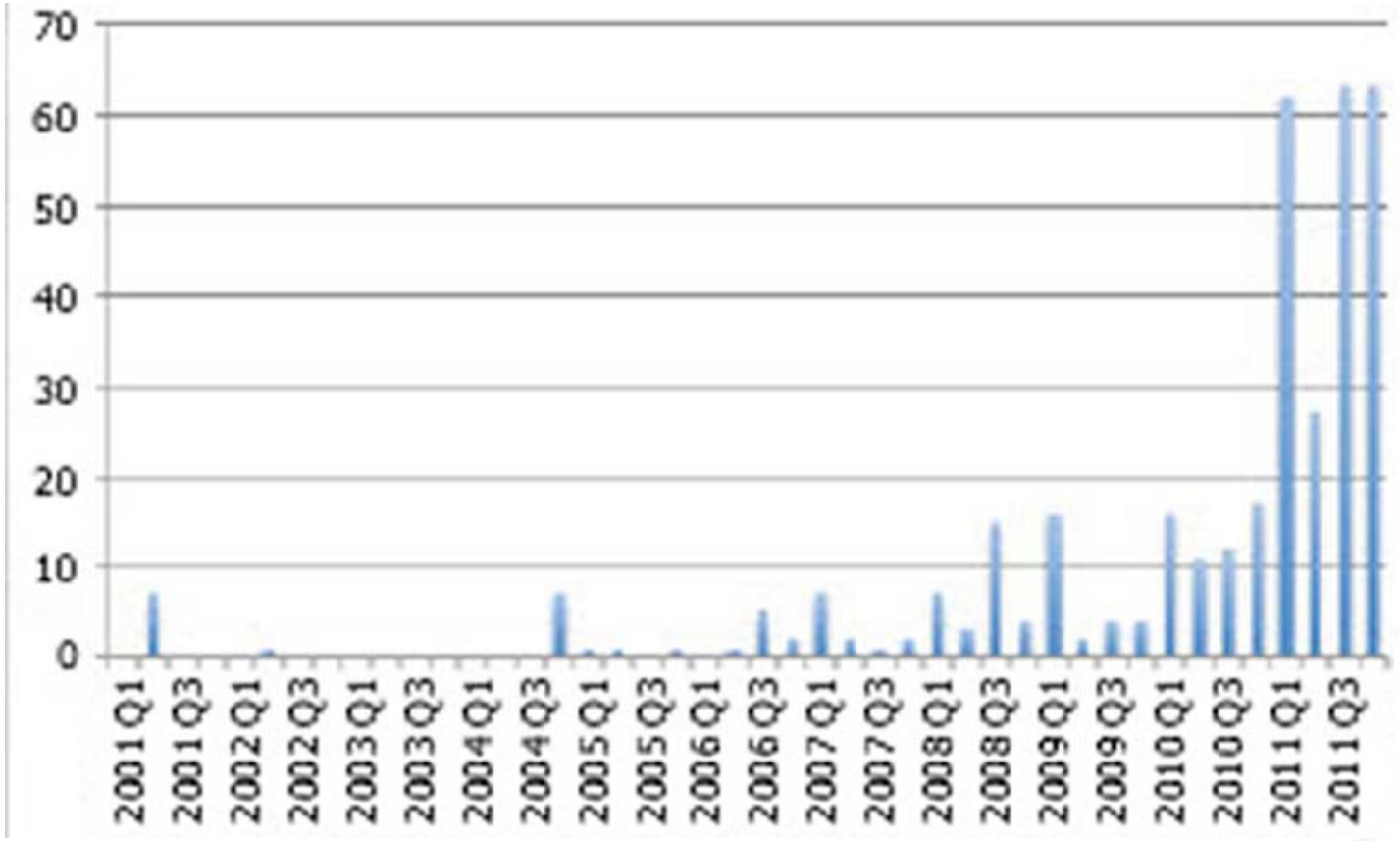
Текущие проблемы безопасности АСУ ТП

- Кто управляет сетью на границе ИТ и АСУ ТП систем?
- Различные требования безопасности в промышленных сетях могут требовать различных уровней безопасности, а также дополнительных аппаратных средств;
- Не своевременное закрытие уязвимостей вендорами;
- Фазинг уязвимостей;
- Одной фильтрации на 502 порту TCP не достаточно(в случае с Modbus/TCP).

Уязвимости на 4 января 2012

- Common Weakness Enumeration: **693** типов уязвимостей
- National Vulnerability Database : **49071** CVE записей
- The Open Source Vulnerability Database : **76958** уязвимостей

ICS-специфичные уязвимости



Количество обнаруженных ICS ориентированных уязвимостей в 2011 году удвоилось по сравнению с предыдущими периодами

Факты и тенденции: системы АСУ ТП

- Объединение с корпоративными сетями;
- Применение бизнес технологий (Ethernet, TCP/IP, *nix системы, сетевые экраны, DMZ’s);
- Web-based SCADA клиенты для доступа к независимому SCADA серверу

Факты и тенденции: сетевые экраны

- Поддержка промышленных протоколов (Modbus/TCP, DNP3, ICCP);
- Многоуровневые системы безопасности (инспектирование пакетов по всей модели OSI);
- Контроль «8 уровня»: логика приложений, включая данные, логику промышленных процессов, безопасность приложений;
- Наличие функция моста (Firewall Bridge) -отсутствие необходимости модифицировать какие либо маршруты или IP адреса;
- Сертификация Modbus IDA;
- Белые и черные списки;
- Возможность распознавать атаки вида «Отказ в обслуживании» и блокировать их (Denial of Service).

Факты и тенденции: шлюзы

- **eWon**
  - Распределенность мониторинга;
  - SCADA и ЦОД eWon централизованы;
  - Отклик для сенсоров даже при отсутствии установленной связи с сервером;
- **WaterFall**
  - Работа в режиме реального времени;
  - Однонаправленность передачи данных исключает возможность манипулирования SCADA из корпоративной сети;
  - Защищённая передача OPC,ICCP, Modbus,DNP3 трафика из промышленной сети в корпоративную;
  - Поддержка сетей с очень большим трафиком;
  - Поддержка кластеров для распределения нагрузок.

Первая IDS for SCADA

Open source SNORT 2.9.2 с поддержкой SCADA

- Поддержка DNP3 and Modbus протоколов;
- Определение аномалий;
- Легкое написание правил;
- Логирование всех ошибок;
- Protocol-Aware Flushing;

Далее

- Больше протоколов;
- Тестовые реализации;
- Расширения команды бета тестеров.

Snort+Cisco ModbusFW

ModbusFW – файрвол с поддержкой протокола Modbus

- Базируется на open source Linux;
- Быстрая фильтрация пакетов на уровне ядра;
- Удобный командный интерфейс Iptables;
- Рост числа использования Linux во встроенных системах и и промышленных компьютерах;

Совместное использование ModBusFW и Snort позволяет построить новую для SCADA инфраструктуру защиты

Виртуальная SCADA HoneyNet от Cisco

- Сбор данных о последних тенденциях и способах взлома;
- Предоставление скриптового индустриального протокола симуляторов для тестирования исходного протокола внедрения;
- Разработка контрмер, таких как «device hardening», «stack obfuscation», сокращение доступной информации о приложениях и эффективный контроль сетевого доступа;

Новые направления специализированных средств защиты информации в АСУ ТП

- Однонаправленность передачи данных
- Глубокий анализ пакетов межсетевыми экранами
- Системы предотвращения вторжений
- Всеобъемлющие интерактивные модели индустриальных процессов

QNX

QNX Neutrino RTOS получил сертификаты безопасности:

IEC 61508 certification at Safety Integrity Level 3 (SIL 3)

ISO/IEC 15408 certification at Evalution Assuarance Level 4+ (EAL 4+)

QNX Сетевые правила

Конфигурирование сетевых правил сетевого экрана QNX очень похоже на конфигурирование в Linux:

- `block in quick from 10.7.0.0/16` – блокировать все пакеты с IP адресов 10.7.0.0 с сетевой маской /16
- `block in quick on ppp0 from 10.7.0.0./16 to any` – пакеты с IP адресов 10.7.0.0 с сетевой маской /16 блокируются если они приходят с интерфейса ppp0
- `block in log quick on en0 proto tcp from any to 20.20.20.0/24 port=23`
- `pass out quick on ppp0 from 20.20.20.0/24 to any` – пропускать пакеты пришедшие с IP адресов с сетевой маской /24
- `Map ppp0 192.168.1.0/24 -> 20.20.20.1/32` конфигурирование NAT

Group-IB

Максим
Паршуков

Инженер по
информационной
безопасности

+7 (495) 661-55-38
parshukov@group-ib.ru
www.group-ib.ru