



Некоммерческое партнёрство
«НАУЧНО-ТЕХНИЧЕСКИЙ СОВЕТ
Единой энергетической системы»

109044 г. Москва, Воронцовский пер., дом 2
Тел. (495) 912-1078, 912-5799, факс (495) 632-7285
E-mail: dtv@nts-ees.ru, <http://www.nts-ees.ru/>

УТВЕРЖДАЮ
Председатель Научно-технической
коллегии НП «НТС ЕЭС», д.т.н.,
профессор

 Н.Д. Роголёв

«13» апреля 2017 г.

ПРОТОКОЛ

заседания секции «Информационные технологии» НП «НТС ЕЭС» по теме:
**«Опытное внедрение на объектах ПАО «МРСК Северо-Запада»
«Вологдаэнерго» Kaspersky Industrial CyberSecurity (KICS)».**

06 апреля 2017 года

№ 1

г. Москва

Присутствовали:
Всего: 12 чел.

Со вступительным словом выступил председатель секции «Информационные технологии», заместитель директора по информационным технологиям Филиала ОАО «СО ЕЭС» Московское РДУ И.А. Щипицин.

С докладом «Опытное внедрение на объекте ПАО МРСК «Северо-Запада» «Вологдаэнерго» KASPERSKY Industrial CyberSecurity (KICS)» выступил эксперт Аналитического отдела АО «РТСофт» Нестеров С.А.

В своём докладе Нестеров С.А. отметил следующее:

1. Объектом внедрения решения была выбрана ПС 110/10кВ Искра Череповецких электрических сетей филиала ПАО «МРСК Северо-Запада» «Вологдаэнерго».

2. Данный пилотный проект является некоммерческим проектом, его целями являются практическая проверка функциональных возможностей решения и отработка технологии внедрения на действующем энергообъекте.
3. Пилотной зоной проекта было определено оборудование телемеханики верхнего уровня (серверы ТМ, БД, АРМ диспетчера) и подсеть телемеханики ПС «Искра».¹
4. Подсистема защиты конечных узлов от угроз ИБ обеспечивает контроль запуска приложений, подключения внешних устройств, сканер уязвимостей, антивирусную защиту, централизованное управление, предотвращение вторжений и межсетевое экранирование.
5. Подсистема мониторинга и выявления инцидентов ИБ в технологических сетях обеспечивает пассивный мониторинг сетей, входящих в состав ТМ, обеспечивая обнаружение подключения новых сетевых устройств, новых/ранее не наблюдавшихся сетевых коммуникаций между узлами сети, обнаружение команд и анализ параметров технологического процесса, передаваемых по протоколу МЭК 61870-5-104²
6. Проектом предусматривалась интеграция решения в защитную инфраструктуру Череповецких электрических сетей для обеспечения возможностей централизованного управления и мониторинга.³
7. Для обеспечения соответствия действующим административно-техническим регламентам заказчика проекта ПАО «МРСК Северо-Запада» был проведён полный комплекс работ по внедрению, включающий в себя предпроектное обследование, разработку, согласование и утверждение необходимой проектной документации, монтажные и пусконаладочные работы, проведение приёмо-сдаточных испытаний и ввод в опытную эксплуатацию.
8. В настоящее время решение находится в опытной эксплуатации, по результатам проведения которой предполагается проведение анализа текущего состояния, а также повышение киберзащищённости объекта путём дальнейшей настройки решения, а также разработки Заказчиком регламентов реагирования на инциденты информационной безопасности.

В обсуждении доклада приняли участие: заместитель директора по информационным технологиям Филиала АО «СО ЕЭС» Московское РДУ Щипицин И.А., заместитель начальника Управления технологических автоматизированных систем и связи Кужеков С.С., директор московского

¹ Приложение к протоколу заседания, слайд «Структурная схема комплекса технических средств».

² Там же, слайды «Журнал событий» и «История событий МЭК 61870-5-104»

³ Там же, слайд «Иерархия управления»

филиала АО «Монитор Электрик» Силков С.В., начальник управления корпоративных автоматизированных систем ПАО «Россети» Хижкин Д.И., начальник аналитического отдела АО «РТСофт» Литвинов П.В., начальник отдела ИТ обеспечения защиты информации ИА АО «СО ЕЭС» Палей Л.М., начальник Службы программно-аппаратных комплексов Филиала АО «СО ЕЭС» ОДУ Центра Глазков А.А., Менеджер по развитию решений по безопасности критической инфраструктуры АО «Лаборатория Касперского» Шипулин А.С.

Отметили:

Для оценки практического применения решения на объектах электроэнергетики следует проанализировать результаты опытной эксплуатации совместно с разработанной нормативно-методологической базой, определяющей регламенты реагирования персонала на инциденты информационной безопасности.

Полный комплекс мероприятий, начинающийся с разработки модели угроз, в данном проекте не применялся, поскольку средство защиты (KISC) было выбрано в начале проекта и одной из целей проекта является определение технической и экономической эффективности использования нового решения в ходе опытной эксплуатации.

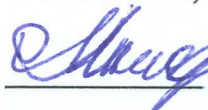
Вопросы обеспечения необходимой перегрузочной способности средства мониторинга киберугроз во внутренней сети объекта не являются критическими для практического применения, поскольку применённые технические решения гарантируют невмешательство средства защиты в работу системы управления технологическим процессом.

Заслушав доклад и выступления участников дискуссии заседания, заседание решило:


1. Принять доклад к сведению.
2. Отметить инновационный характер применённого решения, позволяющего получить ситуационную осведомленность в части фактического состояния информационной безопасности объекта и раннего обнаружения киберугроз.
3. Рекомендовать проанализировать возможность использования информации, содержащейся в файлах описания конфигурации подстанции (SCD) согласно стандарту МЭК 61850-6, с целью автоматизации конфигурирования и настройки решения KICS на объекте.

4. Рекомендовать вернуться к рассмотрению вопроса об эффективности предлагаемого решения по результатам завершения опытной эксплуатации (по согласованию с ПАО «МРСК Северо-Запада»).

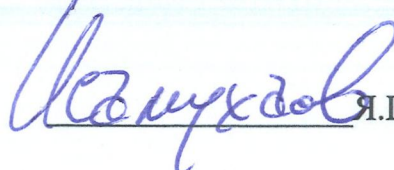
Первый заместитель Председателя
Научно-технической коллегии НП
«НТС ЕЭС», д.т.н., профессор


В.В. Молодюк

Председатель секции
«Информационные технологии»
НП «НТС ЕЭС», заместитель
директора по информационным
технологиям Филиала
АО «СО ЕЭС» Московское РДУ


И. А. Щипицин

Ученый секретарь Научно-технической
коллегии НП «НТС ЕЭС», к.т.н.

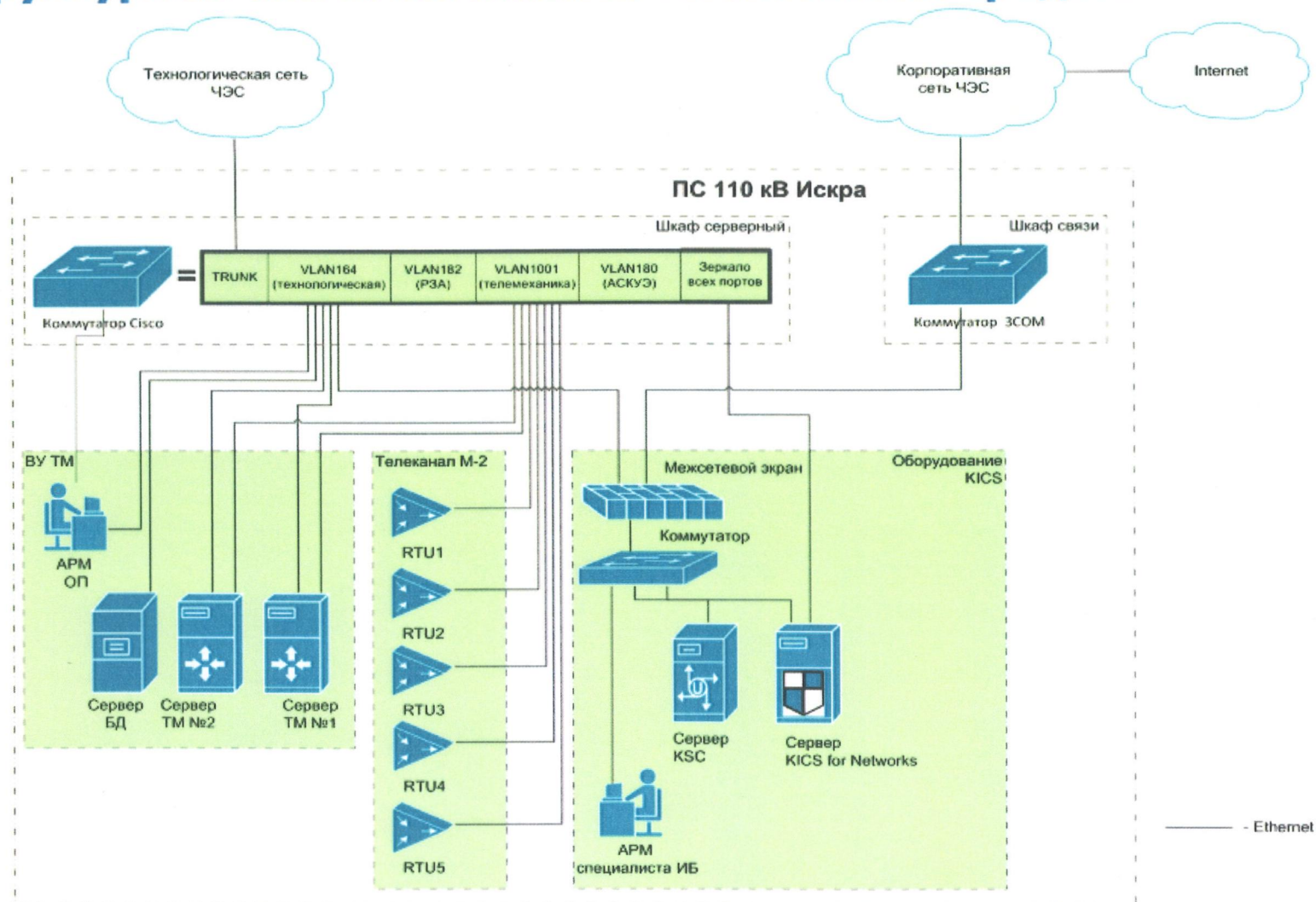

Я.Ш. Исамухамедов

Секретарь секции «Информационные
технологии» НП «НТС ЕЭС»


Е.О. Базилук

Приложение к протоколу заседания секции «Информационные технологии» НП «НТС ЕЭС» по теме: «Опытное внедрение на объектах ПАО «МРСК Северо-Запада» «Вологдаэнерго» Kaspersky Industrial CyberSecurity (KICS)».
Слайды из презентации.

Структурная схема комплекса технических средств



Слайд «Структурная схема комплекса технических средств»

Applications Places Kaspersky Industrial CyberSecurity for Networks Console Fri 12:34

Kaspersky Industrial CyberSecurity for Networks

Управление политикой безопасности Управление Сервером и сенсорами Параметры Консоли Помощь

События: 81 История событий Технологические параметры **Настройка**

01:18:05.890 14-12-2016 **Контроль целостности сети:**
Обнаружен неизвестный узел в сети. MAC-адрес: 68:7B:BC:A6:37:03 IP-адрес: 10.183.49.120 порт: 59874

01:16:45.920 14-12-2016 **Контроль целостности сети:**
Обнаружено неразрешенное сетевое взаимодействие по протоколу: TCP

01:16:45.920 14-12-2016 **Контроль целостности сети:**
Обнаружен неизвестный узел в сети. MAC-адрес: 68:7B:BC:A6:37:03 IP-адрес: 10.183.49.120 порт: 59874

01:05:55.740 14-12-2016 **Контроль целостности сети:**
Обнаружено неразрешенное сетевое взаимодействие по протоколу: UDP

Информация о событии

| Уровень важности | Важные | Описание |
|------------------|---------------------------|--|
| Категория | Контроль целостности сети | Обнаружено неразрешенное сетевое взаимодействие. Протокол: TCP |
| Идентификатор | 3532407 | Источник: MAC-адрес: 68:7B:BC:A6:37:03 IP-адрес: 10.183.49.120, порт: 59874 Получатель: MAC-адрес: 68:7B:BC:A6:37:03 IP-адрес: 10.183.49.120, порт: 49.34 |
| Обнаружено | 01:16:45.920 14-12-2016 | Точка мониторинга: mpoint1 |

Журнал событий

Событие подтверждено

Трафик: 266 кбит/сек. Теги: 0 тегов/сек.

Создать правило контроля сети Подтвердить Закрыть

Слайд «Журнал событий»

События 81

История событий

Технологические параметры

Настройка

Уровень важности: Все Категория: Все Применить

Период: 12-12-2016 23:59:59 - 14-12-2016 23:59:59 Включая подтвержденные Выбрано событий: 15317

| Уровень важности | Обнаружено | Категория | Заголовок |
|------------------|-------------------------|-------------------------------|---|
| Важные | 03:24:36.150 13-12-2016 | Контроль целостности процесса | Протокол Iec104 Обнаружена команда группового опроса данных (INTERROGATION) |
| Важные | 03:24:38.56 13-12-2016 | Контроль целостности процесса | Протокол Iec104 Обнаружена команда группового опроса данных (INTERROGATION) |
| Важные | 03:24:39.960 13-12-2016 | Контроль целостности процесса | Протокол Iec104 Обнаружена команда группового опроса данных (INTERROGATION) |
| Важные | 03:24:43.180 13-12-2016 | Контроль целостности процесса | Протокол Iec104 Обнаружена команда группового опроса данных (INTERROGATION) |
| Важные | 03:28:31.690 13-12-2016 | Контроль целостности процесса | Протокол Iec104 Обнаружена команда группового опроса данных (INTERROGATION) |

Информация о событии

| | | |
|------------------|-------------------------------|---|
| Уровень важности | Важные | Описание |
| Категория | Контроль целостности процесса | Обнаружена команда группового опроса данных (INTERROGATION). Объект: 3 |
| Идентификатор | 3532187 | Протокол Iec104 |
| Обнаружено | 03:24:36.150 13-12-2016 | Устройство КП-30 |
| | | Источник MAC-адрес 04:00:58:56:22:b7; IP-адрес 188.358.350:81 порт 518888 |
| | | Получатель MAC-адрес 00:50:56:22:22:22; IP-адрес 188.358.350:81 порт 518888 |

Select events

- IEC 60870-5-104
 - END OF INITIALIZATION
 - INTERROGATION
 - COUNTER INTERROGATION
 - CLOCK SYNCHRONIZATION
 - RESET PROCESS ACTIVATION
 - RESET PROCESS CONFIRMATION
 - PARAMETER ACTIVATION
 - CALL DIRECTORY, SELECT FILE, CALL FILE, CALL SECTION
 - START DATA TRANSFER (STARTDT)
 - STOP DATA TRANSFER (STOPDT)
 - WRITE: UNKNOWN ADDRESS
 - TEST
 - READ
 - TEST WITH TIME TAG
 - DELAY ACQUISITION
 - UNEXPECTED SEND SEQUENCE NUMBER
 - UNEXPECTED RECEIVE SEQUENCE NUMBER
 - UNKNOWN COMMAND
 - UNKNOWN SUBCOMMAND
 - WRONG PACKET SIZE
 - WRONG PACKET FORMAT
 - PARSER: BUFFER NOT VALID

OK Cancel

История событий: контроль целостности процесса

Событие подтверждено

Трафик: 379 кбит/сек. Теги: 0 тегов/сек

Слайд «История событий протокола МЭК 61870-5-104»

Kaspersky Security Center 10

Файл Действие Вид Справка

Управляемые компьютеры

Сервер администрирования - ПС Искра > Управляемые компьютеры

Клиентские компьютеры

Компьютеры Политики Задачи [Параметры группы](#)

Добавить компьютеры Создать группу Выполнить действие [Добавить или удалить графы](#) [Обновить](#)

Фильтр не задан, всего записей: 3

Выбрать статусы: Критический: 1 Предупреждение: 1 ОК: 5 (включая подгруппы) [Поиск по текстовым графам](#)

| Имя | Описание | Тип операционной системы | Домен | Устан |
|---------------------------|----------|----------------------------------|-----------|-------|
| Kaspersky Security Center | | Microsoft Windows Server 2012 R2 | WORKGROUP | ✓ Да |
| KICS for Networks 1.4 | | Linux | MYGROUP | ✓ Да |
| SECURITY-PC | АРМ ИБ | Microsoft Windows 7 | WORKGROUP | ✓ Да |

Групп: 2, компьютеров: 7

Справка KASPERSKY

KSC: иерархия управления

Слайд «Иерархия управления»