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. Рогалёв

«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 61870-5-104[2]

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.

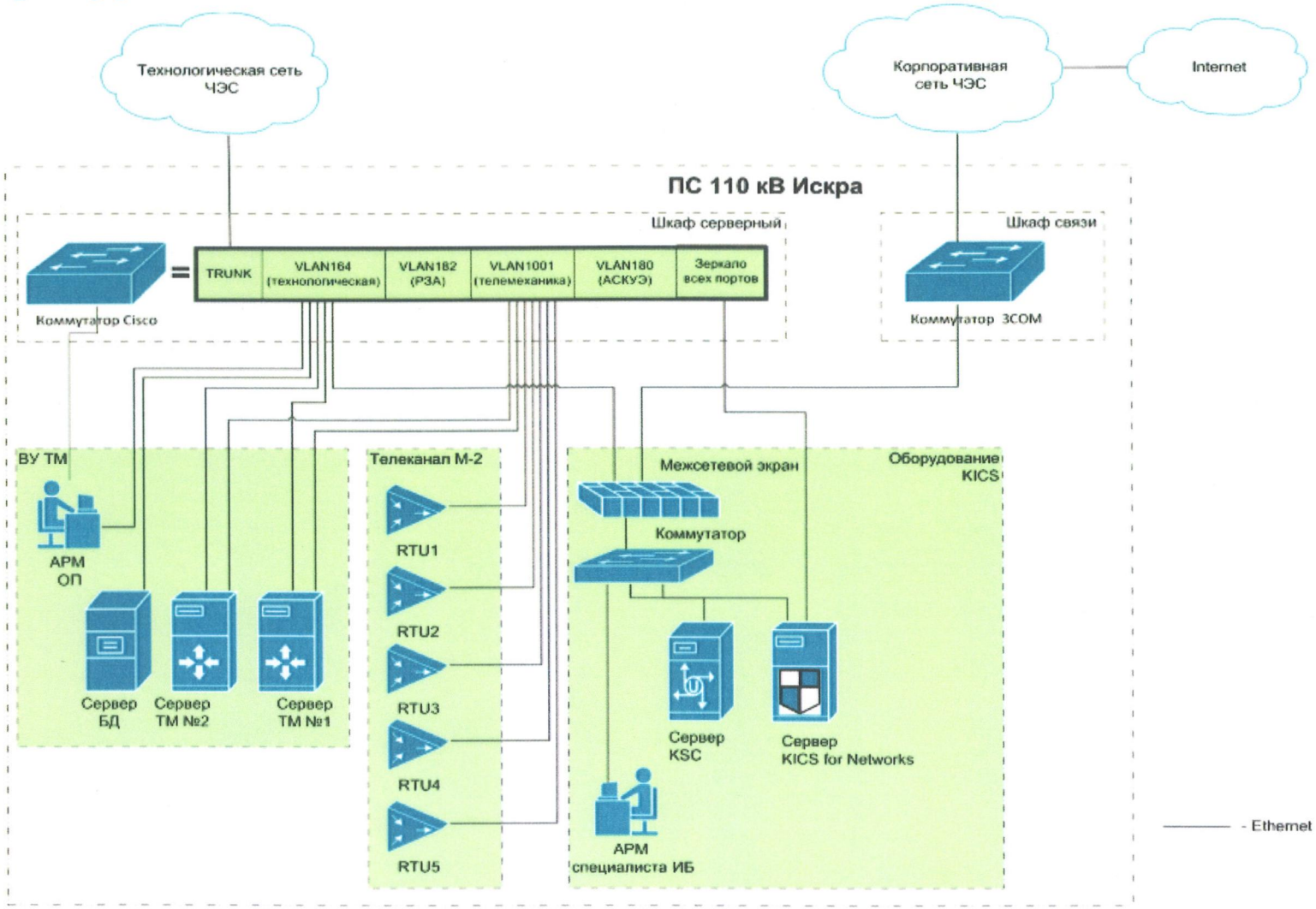
_____ Я.Ш. Исамухамедов

Секретарь секции «Информационные технологии» НП «НТС ЕЭС»

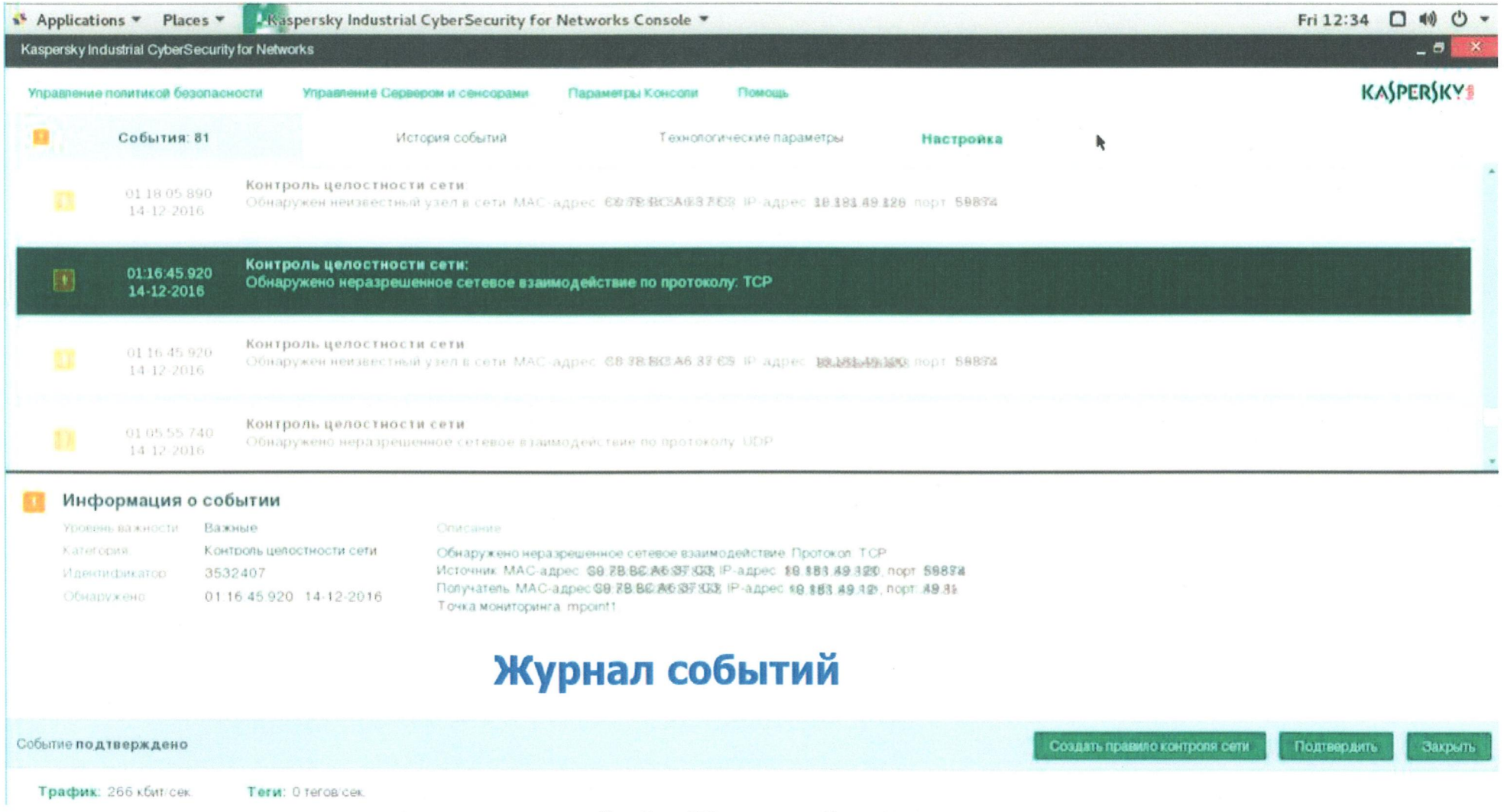
_____ Е.О. Базилюк

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.

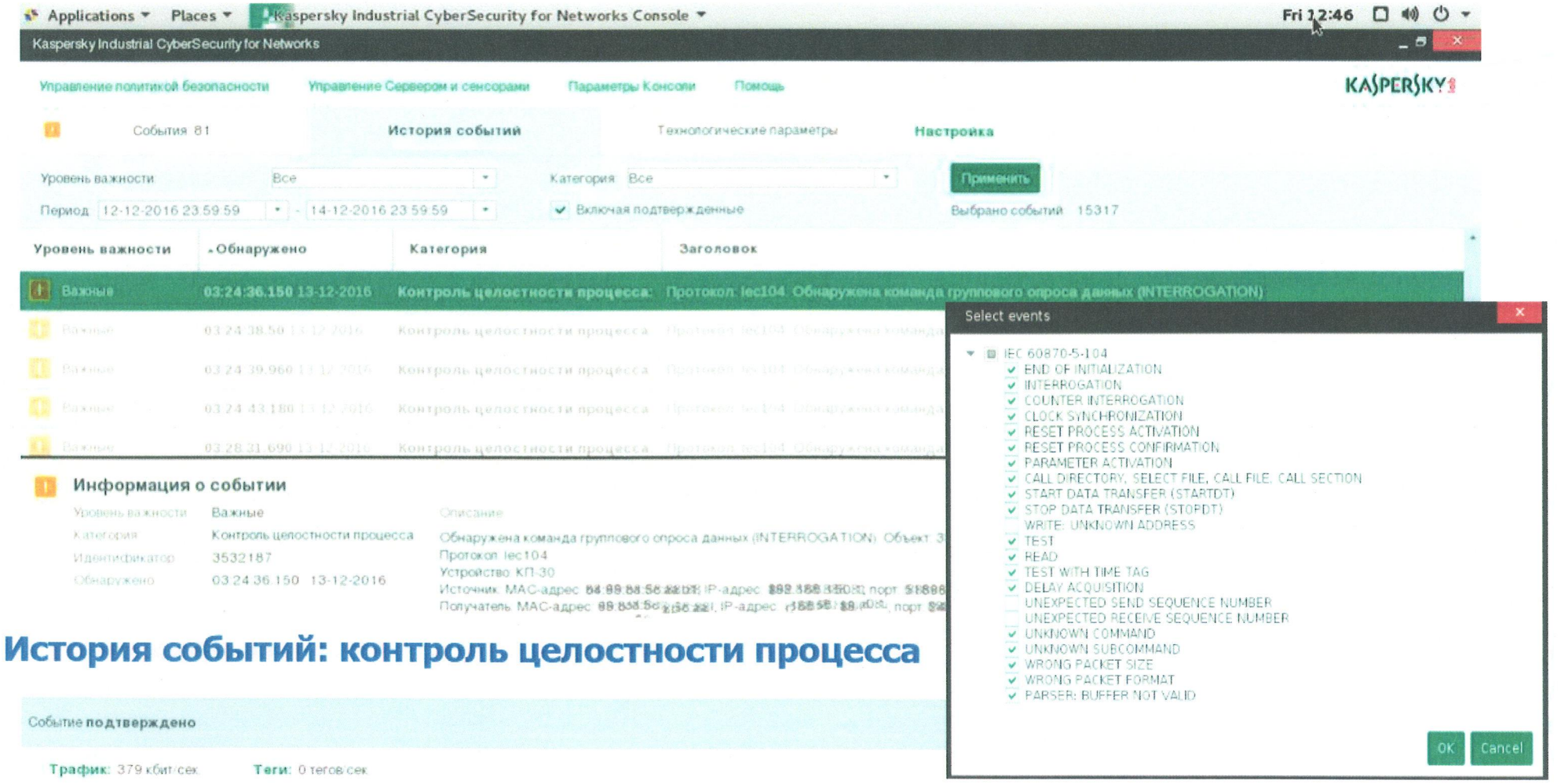
Структурная схема комплекса технических средств



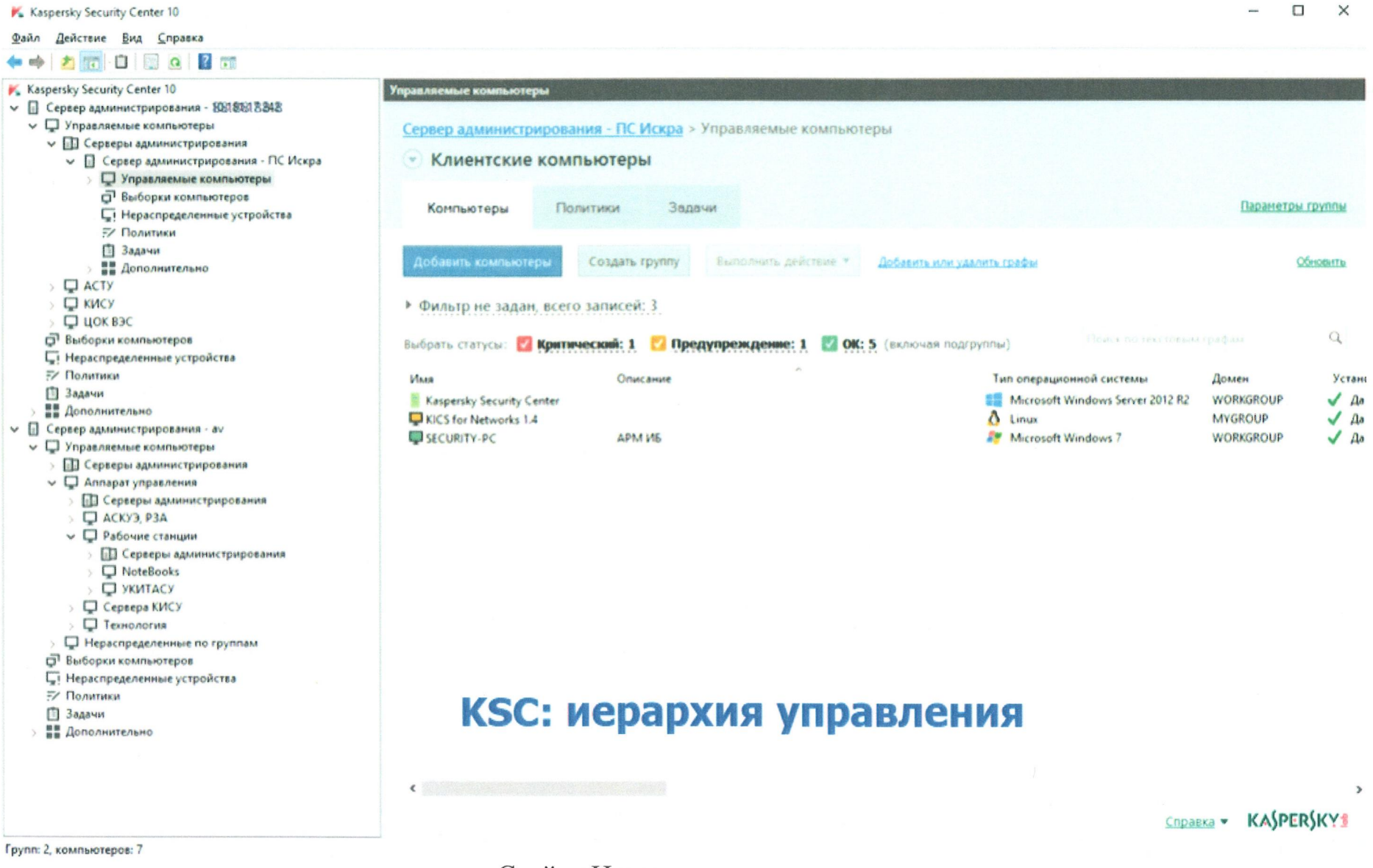
Слайд «Структурная схема комплекса технических средств»



Слайд «Журнал событий»



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



Слайд «Иерархия управления»