КРИПТОСОФТ
НАУЧНО-ТЕХНИЧЕСКОЕ ПРЕДПРИЯТИЕ

Интеграция защищённой операционной системы QP ОС в доменную инфраструктуру

Докладчик: Баринов А. Д.

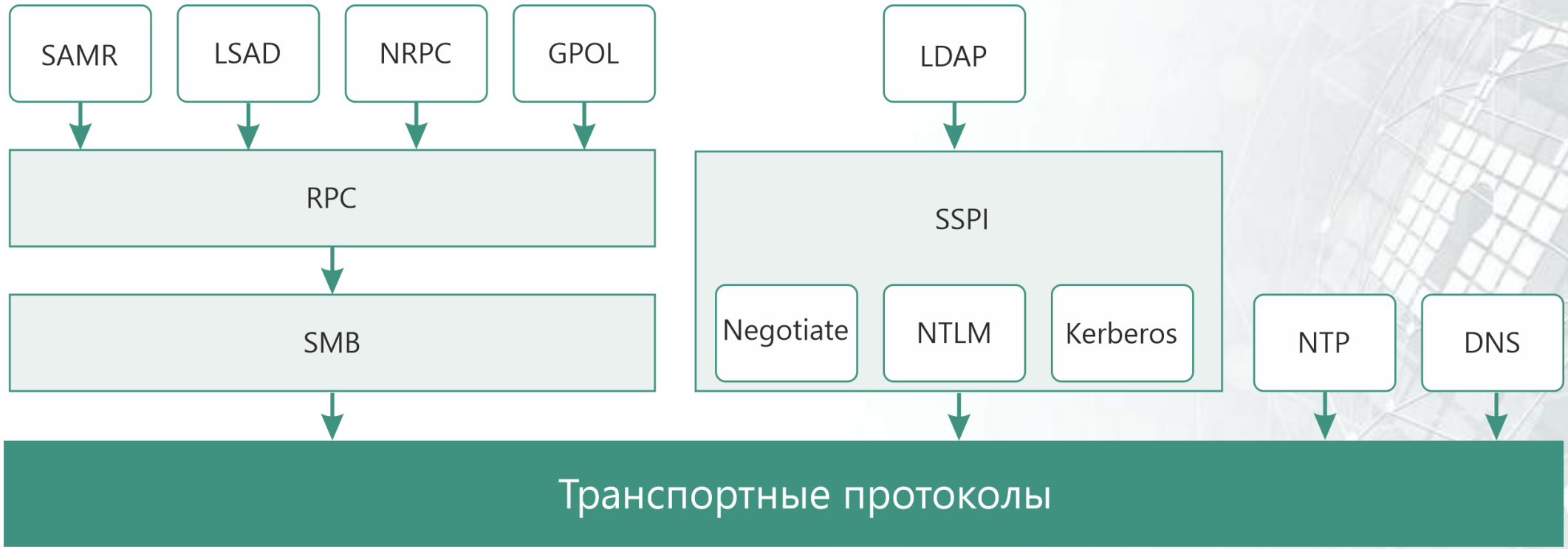
Преимущества доменной инфраструктуры

- Централизованное управление учетными записями
- Единая точка аутентификации
- Единая точка управления политиками
- Повышенный уровень информационной безопасности

Требования для интеграции в домен

- В операционной системе рабочей станции должны быть установлены соответствующие **компоненты**
- У машины должен быть сконфигурирован **сетевой интерфейс**, через который будет выполняться доступ к КД
- **Межсетевой экран** должен быть настроен таким образом, чтобы сетевые пакеты протоколов, используемых для работы в домене не блокировались
- Время рабочей станции должно быть **синхронизировано** с КД

Протоколы взаимодействия с доменом



Протоколы аутентификации

Kerberos и **NTLM**:

- Интерактивный вход доменным пользователем
- Сетевой вход доменным пользователем
- Смена пароля доменного пользователя
- Обеспечение целостности и конфиденциальности
- Поддержка SSPI

Реализация протокола Kerberos в QP ОС

Статическая библиотека:

- Разбор и построение пакетов протокола (AS, TGS, AP, PRIV, CRED, ERROR)
- Шифрование и подсчёт контрольных сумм

Динамическая библиотека:

» Интерактивный вход доменного пользователя в систему

» Генерация запроса аутентификации к серверу приложения с предварительной аутентификацией на КД и получением служебного билета

» Смена пароля доменного пользователя

Динамическая библиотека поставщика поддержки безопасности:

- Согласование контекста безопасности
- Шифрование, дешифрование, подпись и проверка подписи сообщений

Облегчённый протокол доступа к каталогам LDAP

Прототипы функций, экспортируемых динамической библиотекой реализации протокола LDAP в QP ОС, идентичны прототипам функций библиотеки Wldap32.dll

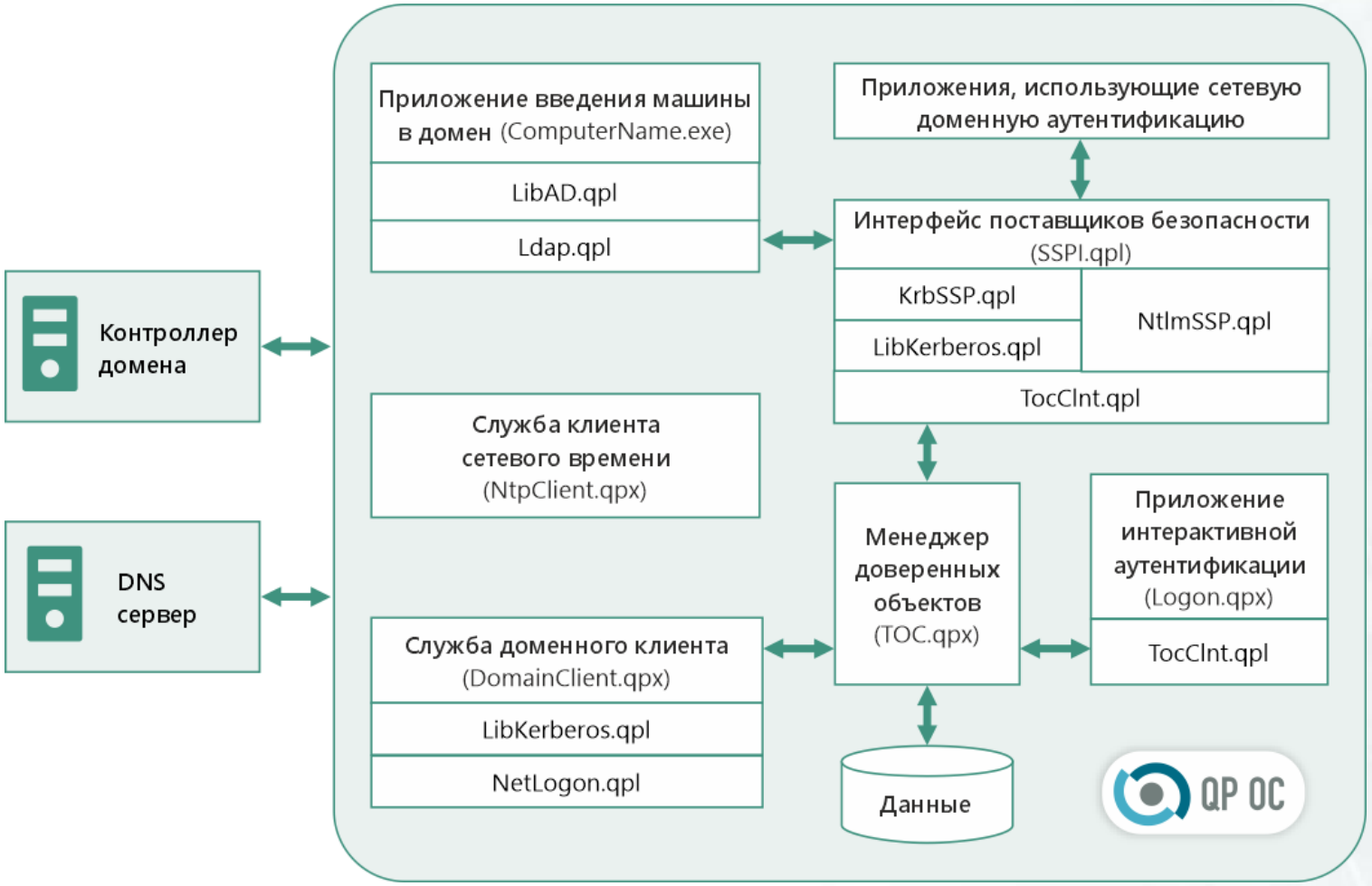
Сценарии использования протокола в QP ОС:

- Создание на КД аккаунта компьютера
- Изменение атрибутов доменных учётных записей
- Получение списка доменных групп и пользователей
- Получение места расположения групповых политик

Другие протоколы

- Протокол дистанционного **диспетчера учётных записей безопасности** SAMR
- Дистанционный протокол **локального органа безопасности** LSAR
- Протокол сетевой **аутентификации** Netlogon
- Основной протокол **групповой политики** GPOL
- Протокол **сетевого времени** NTP

Схема компонентов доменного взаимодействия QP ОС



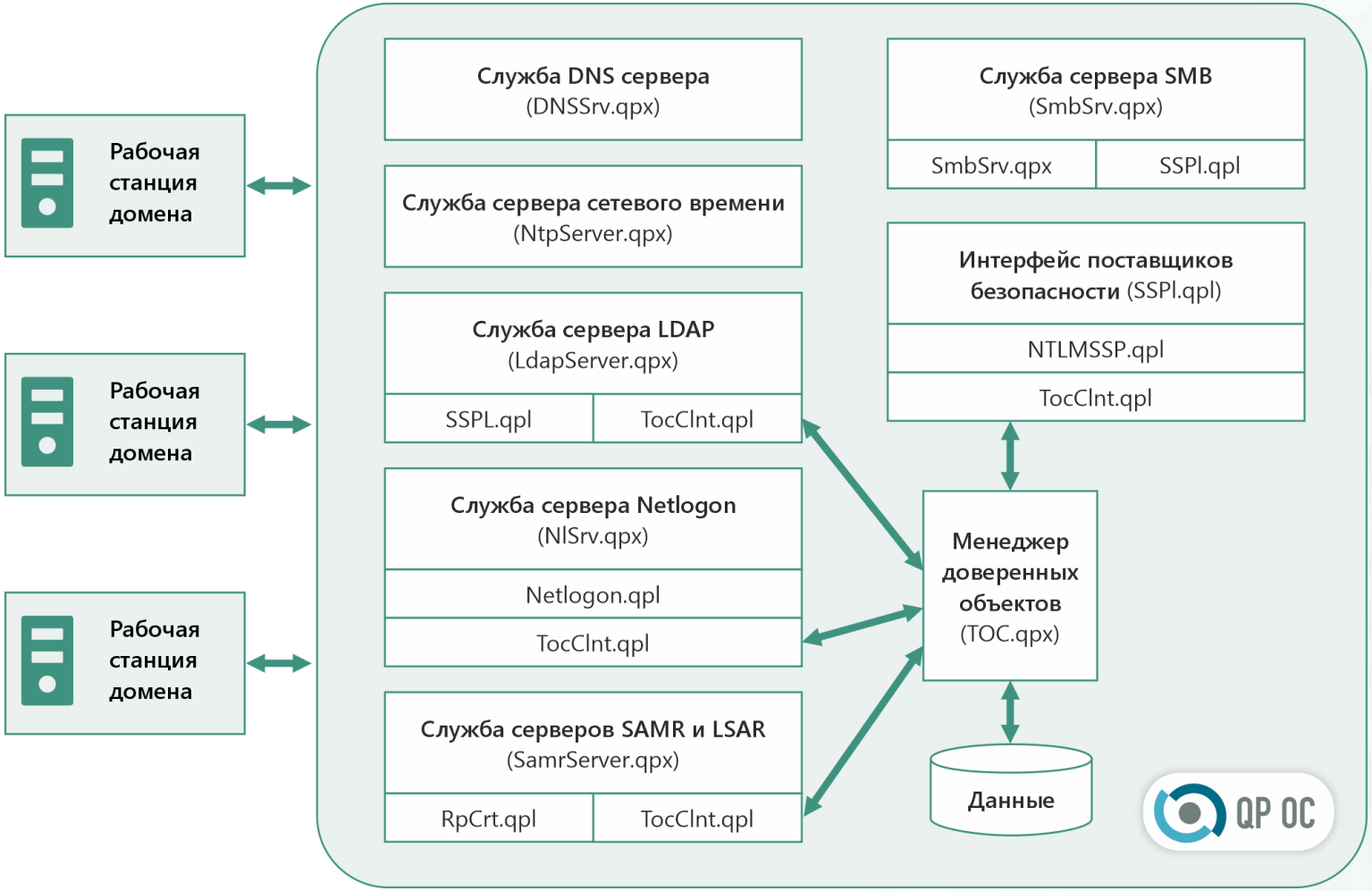
Информационные потоки между узлами домена

- Потоки управления доменом
- Файловый обмен
- Web-трафик
- Трафик СУБД
- Потоки дистанционного управления доступом
- Почтовый обмен

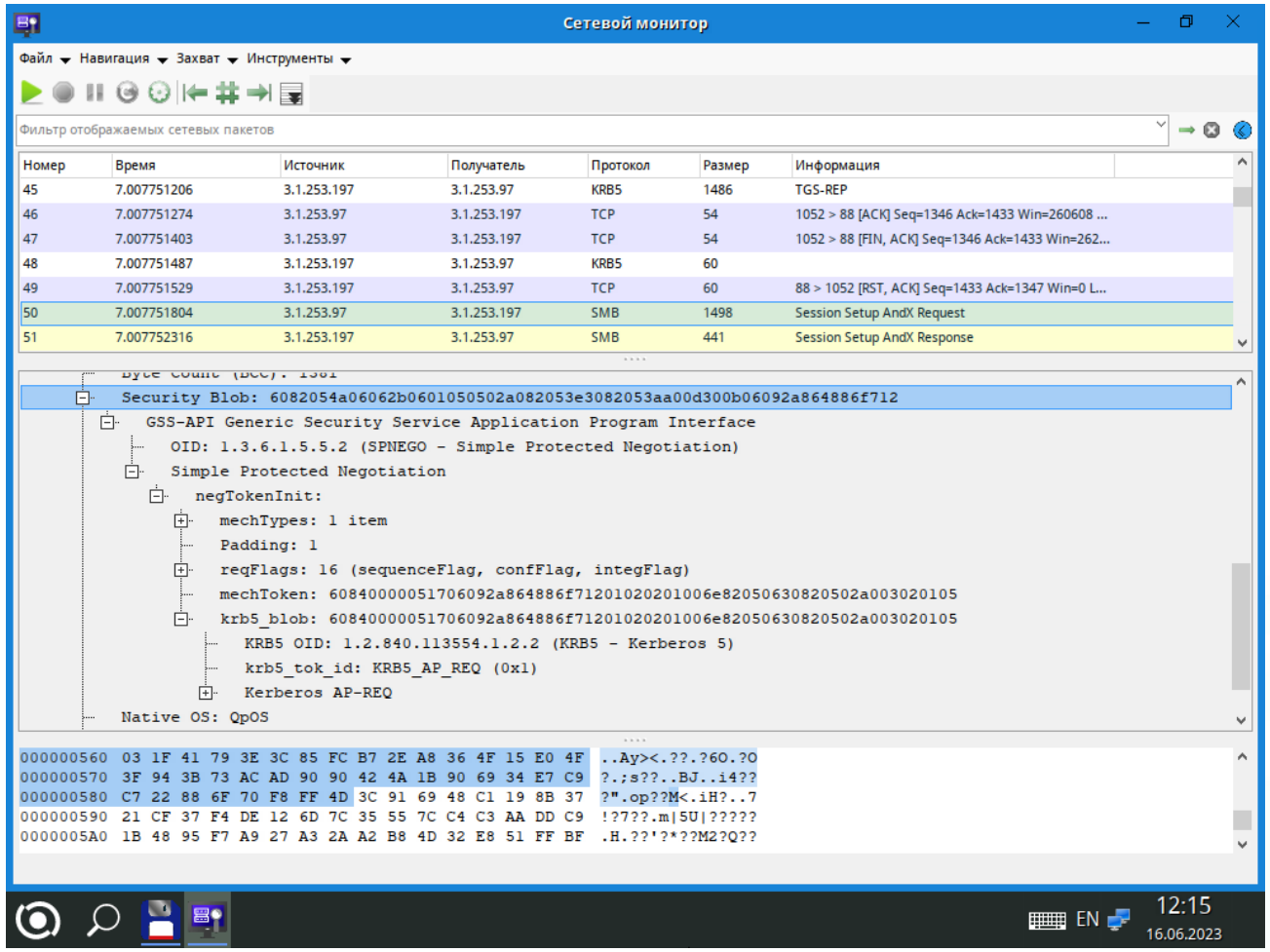
Роли контроллера домена под управлением QP ОС

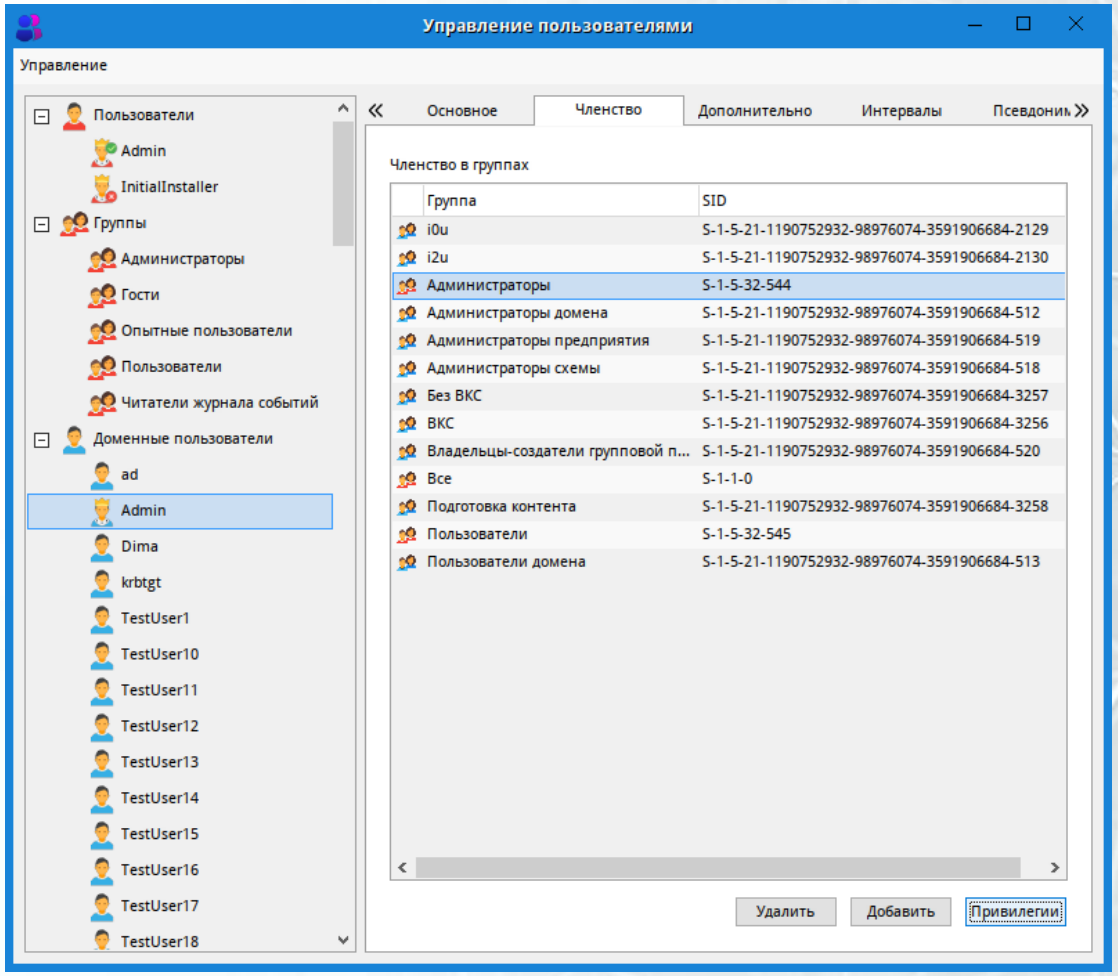
- Роль сервера **облегчённого протокола доступа к каталогам** LDAP
- Роль сервера **службы доменных имён** DNS
- Роль сервера **сетевого времени** NTP
- Роль сервера **аутентификации** Netlogon
- Роль сервера дистанционного **диспетчера учётных записей безопасности** SAMR
- Роль сервера дистанционного протокола **локального органа безопасности** LSAR
- Роль сервера **дистанционного доступа к файлам** SMB

Схема модулей КД QP ОС



Процесс разработки





Процесс тестирования

- Разработка нагрузочных и функциональных **тестов**
- Использование **статических анализаторов**
- Использование **опций компилятора** (RunTimeCheck /RTCsu, Buffer Security Check /GS)
- Профилирование использования **памяти**

Дальнейшее развитие

- Реализация **серверной службы билетов** Kerberos
- Реализация **доверительных отношений в доменах**
- Интеграция с **сервером обновлений** операционной системы QP ОС
- Автоматическое обновление **антивирусных баз** в рамках домена
- Интеграция с СХД (**системы хранения данных**)

КРИПТОСОФТ
НАУЧНО-ТЕХНИЧЕСКОЕ ПРЕДПРИЯТИЕ

Спасибо за внимание!

www.cryptosoft.ru

qpos@cryptosoft.ru