Технологии QNX и КПДА в России

Особенности сертификации автоматизированных систем специального назначения на базе КПДА и QNX

Тимур Белкин, Виктор Пайгусов
Центр защиты информации АО «НИИ «Вектор»

СВД Встраиваемые Системы

Обзор требований по сертификации по требованиям безопасности информации

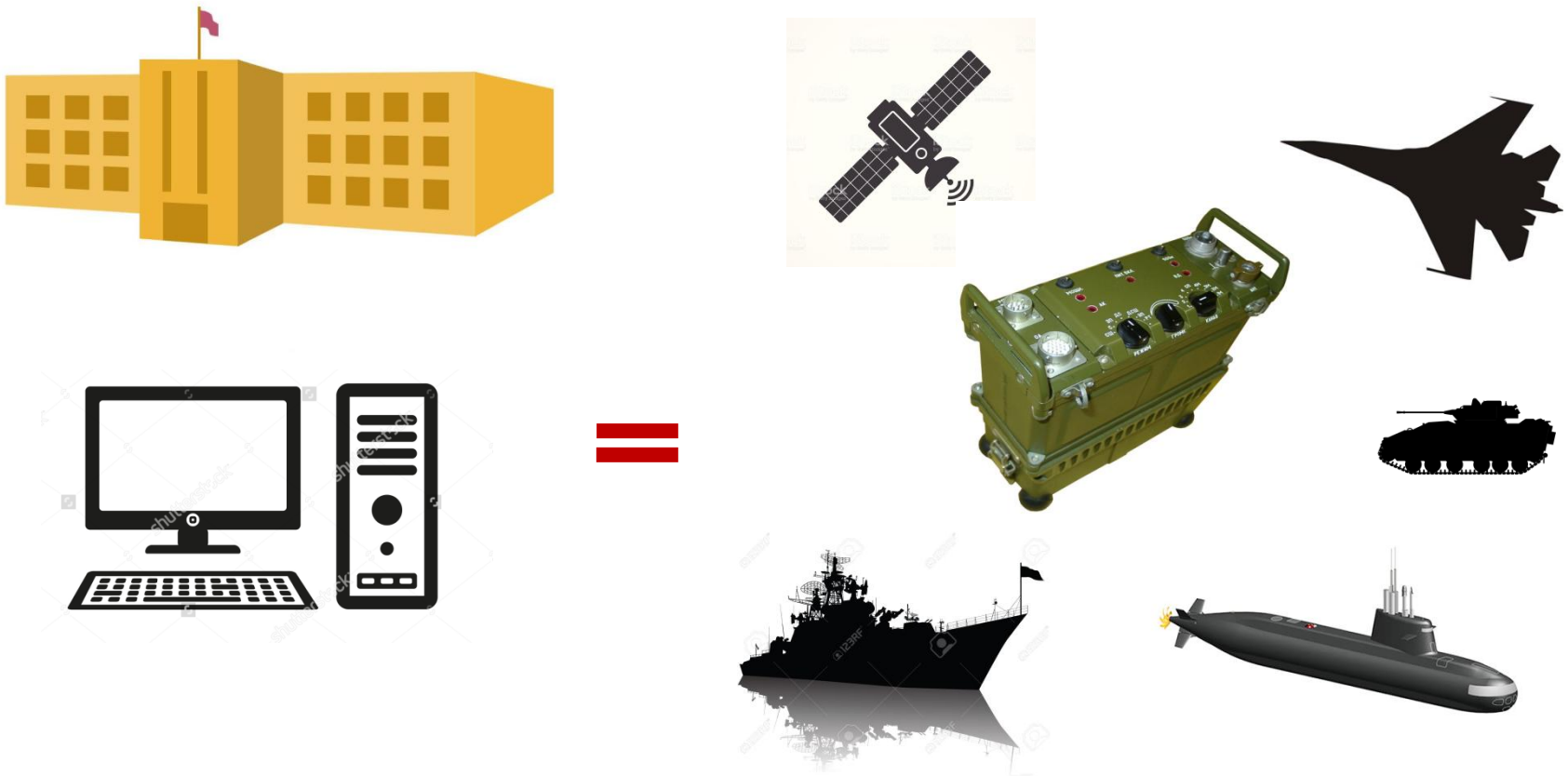
Общие требования ко всей АС

РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992 г.)

Частные требования к СЗИ

Для всех СЗИ	Для СЗИ НСД (Включая ОС)	Для межсетевых экранов	Для генераторов паролей	Для средств антивирусной защиты	Для систем обнаружения вторжений
РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999)	РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992)	РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997)	Требования МО России к датчикам случайных чисел и системам паролирования	«Требования к средствам антивирусной защиты» (ФСТЭК России, 2012)	«Требования к системам обнаружения вторжений» (ФСТЭК России, 2011)
	«Требования безопасности информации к операционным системам» (ФСТЭК России, 2016)	«Требования к межсетевым экранам» (ФСТЭК России, 2016)			

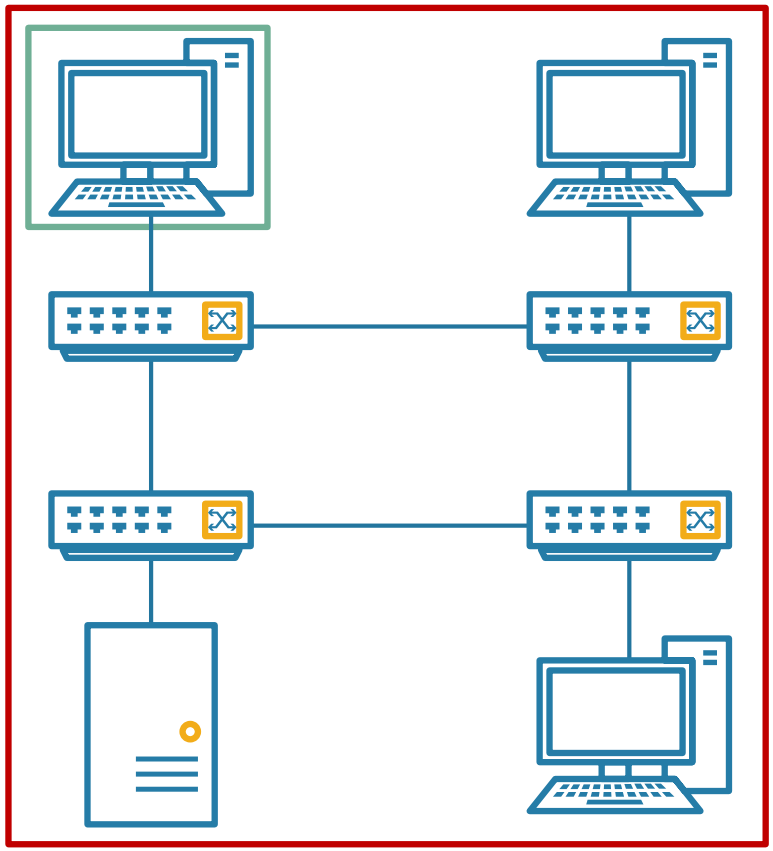
Сертификация является обязательной для любых изделий военного назначения, используемых для обработки защищаемой информации.



При этом требования <u>не дифференцированы</u> по типам Изделий и <u>не учитывают</u> особенностей эксплуатации Изделий.

Вопросы сертификации по требованиям безопасности информации

Фактическая обработка защищаемых сведений



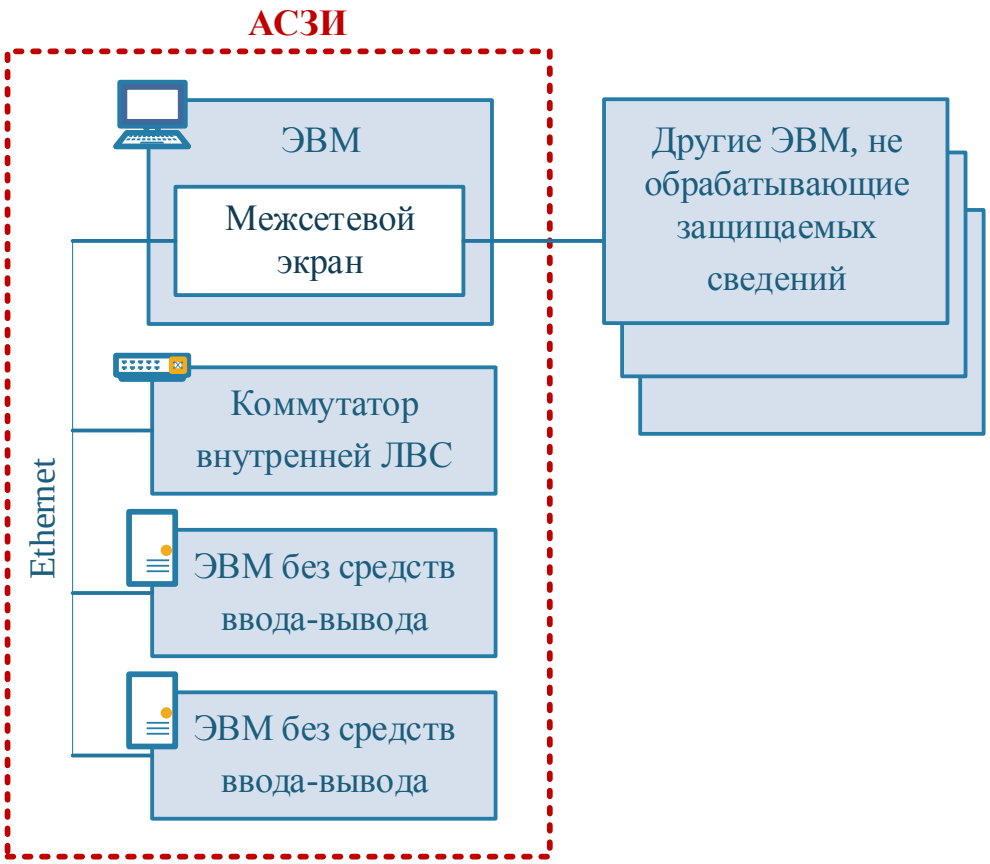
Предъявление требований

Без сегментирования автоматизированной системы:

–требования предъявляются исходя из наивысшего уровня защищенности;

–требования предъявляются ко всем ЭВМ, соединенным линиями связи, независимо от фактической обработки на них защищаемых сведений.

Объект защиты



Объект защиты:

– содержит ЭВМ, обрабатывающие защищаемые сведения, и ЭВМ, не обрабатывающие защищаемые сведения;

– содержит ЛВС;

– требует централизованного управления СЗИ НСД, т.к. содержатся ЭВМ, не оснащенные средствами ввода-вывода.

От сертификата на ОС до сертификата на Изделие

на базе ЗОСРВ «QNX» КПДА.00002-01

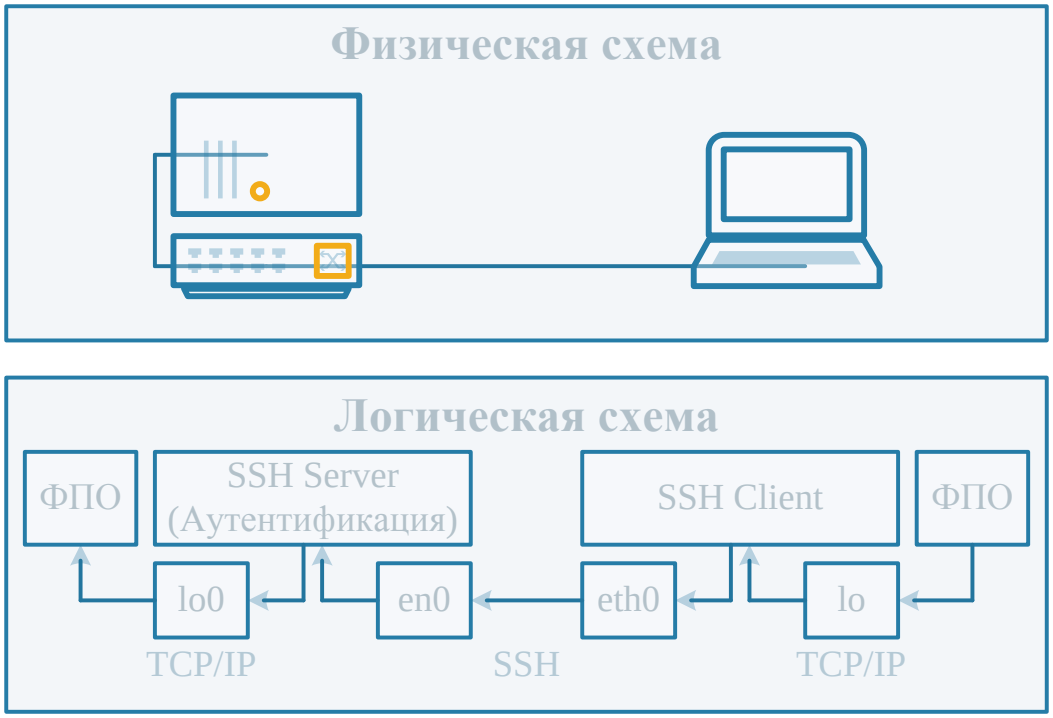
Применение средств защиты с действующим сертификатом	Подготовка к сертификации	Сертификация
Применение ЗОСРВ «QNX» КПДА.00002-01 в качестве средства защиты информации от НСД	Применение дополнительных технических решений на базе ЗОСРВ «QNX» КПДА.00002-01 для учета особенностей эксплуатации Изделий; Настройка и доработка механизмов МЭ в ЗОСРВ «QNX» КПДА.00002-01 для выделения ЭВМ, не обрабатывающих защищаемой информации, за пределы контура обработки защищаемой информации	При необходимости сегментации АС в защищенном исполнении требуется использование аппаратных МЭ или сертификация программных механизмов КПДА на соответствие действующим требованиям к МЭ

От сертификата на ОС до сертификата на Изделие

на базе ЗОСРВ «Нейтрино» КПДА.10964-01

Применение средств защиты с действующим сертификатом	Подготовка к сертификации	Сертификация
Применение ЗОСРВ «Нейтрино» КПДА.10964-01 в качестве средства защиты информации от НСД, межсетевого экрана, оснастки администратора (возможно частичное централизованное управление СЗИ НСД встроенными средствами)	Применение дополнительных технических решений на базе ЗОСРВ «Нейтрино» КПДА.10964-01 для учета особенностей эксплуатации Изделий; Настройка МЭ для выделения ЭВМ, не обрабатывающих защищаемую информацию, за пределы контура обработки защищаемой информации	При сертификации в составе Изделия выделяется АС в защищенном исполнении, которая ограничена только контуром обработки защищаемой информации (остальные узлы в состав объекта сертификации не включаются) Требования к АСЗИ реализуются применением штатных средств ЗОС РВ и дополнительных технических решений

Решения по идентификации и аутентификации

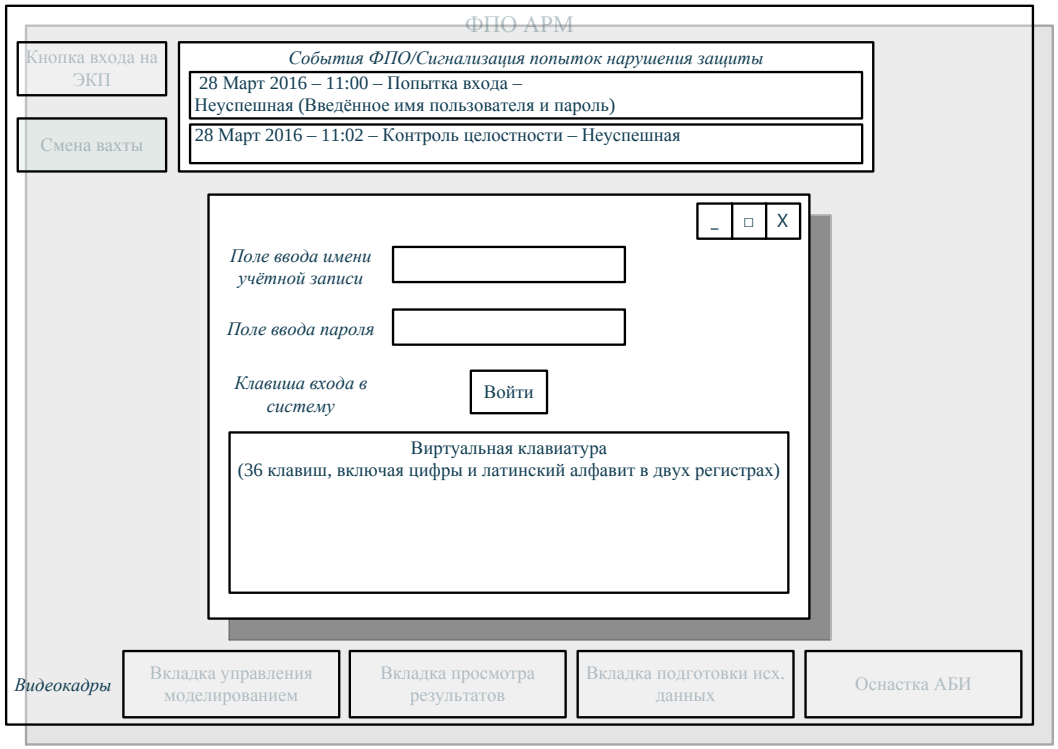


В Изделиях применяют ноутбуки для считывания информации из функционального ПО через сетевой сокет.

Механизмов ОС не достаточно для полного выполнения требований по аутентификации на уровне сокета.

Существует решение, основанное на запуске функционального ПО на локальной петле ОС и применении “проксирования” и аутентификации к сокету ФПО средствами SSH (Решение базируется на штатных модулях ОС)

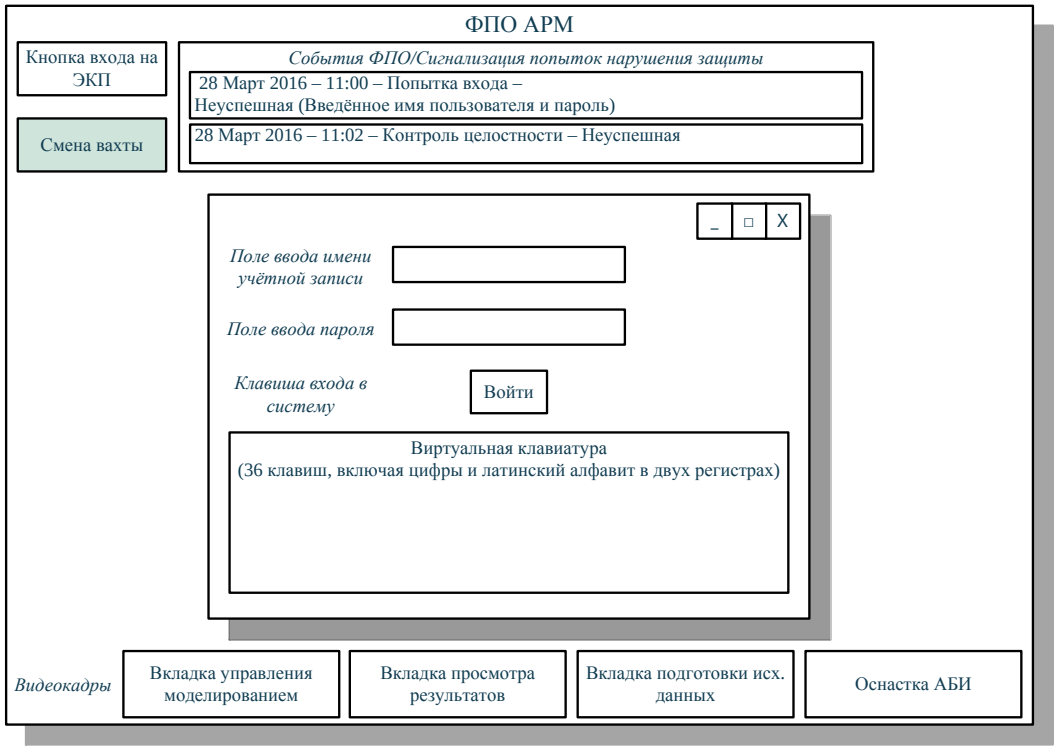
Решения по дискреционному разграничению доступа



В изделиях может быть реализована смена пользователя и применение прав доступа при смене вахты, с учетом необходимости непрерывной и бесперебойной работы изделия

Разработано решение по реализации дискреционного и мандатного управления доступа в ФПО. Смена пользователя при этом возможна без выхода из системы, также предусмотрена учетная запись с ограниченными правами для входа в экстренной ситуации без пароля

Решения по дискреционному разграничению доступа



При этом применение КПДА является обязательным:

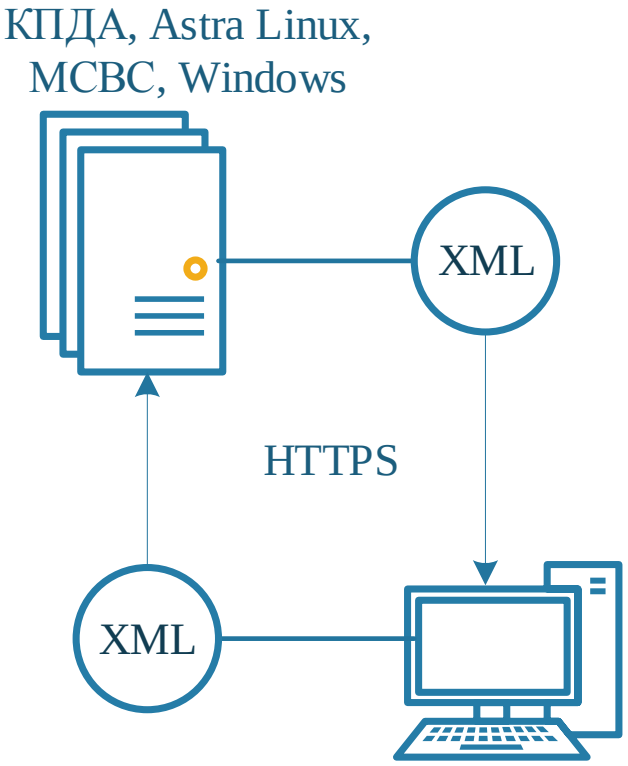
1) КПДА предоставляет безопасный API (в наложенных СЗИ НСД может возникнуть ситуация, что часть API будет безопасным, т.к. оно предоставляется СЗИ, а часть небезопасным, т.к. оно предоставляется несертифицированной ОС).

2) КПДА реализует другие механизмы безопасности, для снижения требований к ФПО.

Решения по безопасному освобождению неиспользуемых областей памяти

ОС применяются на объектах, в отношении которых действуют дополнительные требования: - по экстренному уничтожению информации; - исключению доступа служб эксплуатации (представителей промышленности) к оперативной информации. (Требования проверяются как при сертификации, так и при предъявлении Изделия Заказчику по требованиям ТЗ)	Для реализации дополнительного требования разработано решение по: - размещению защищаемой информации на ram-диске (в оперативной памяти); - установке необходимых дискреционных прав и мандатных меток к данным ресурсам; - очистке оперативных данных при отключении питания. (Решения базируются на применении штатных модулей ЗОСРВ QNX с минимальной дработкой функционального ПО)

Решения по централизованному управлению СЗИ НСД в разнородных средах



При использовании в изделии КПДА с другими ОС может потребоваться применение решений по централизованному управлению СЗИ НСД

Одним из решений является использование оснасток на базе протокола XML-RPC:

1) Оснастка позволяет выполнять смену паролей, просмотр журналов регистрации, контроль целостности.
2) Возможно использование как API СЗИ НСД, так и командной оболочки.

Технологии QNX и КПДА в России

Спасибо за внимание!

Тимур Белкин, Виктор Пайгусов
Центр защиты информации АО «НИИ «Вектор»

+7 (812) 234-37-02; t.g.belkin@czsp.ru

СВД Встраиваемые Системы