

ПК ФАНТОМ

Текущее состояние и
перспективы

(облачная платформа)

Содержание

1. Назначение
2. Подход и преимущества ПК Фантом
3. Текущее состояние. Функциональность
4. Сертификация
5. Развитие ПК Фантом
6. Варианты и примеры использования

Назначение

- ❖ ПК ФАНТОМ - программное средство, предназначенное для создания защищенного рабочего места на базе персонального компьютера
- ❖ ПК ФАНТОМ позволяет значительно упростить организационно-технические меры защиты информации

Подход и преимущества ПК «ФАНТОМ»

- ❖ ПК Фантом устанавливается на персональный компьютер с целью контроля работы разворачиваемых ОС, периферийных устройств, сетевого взаимодействия, а также прикладного окружения пользователя
- ❖ Работа на компьютере с ПК Фантом для пользователя практически не отличается от его работы на стандартном рабочем месте с MS Windows, кроме возможности работы с несколькими рабочими местами на одном компьютере, и повышенных мер безопасности
- ❖ Требования доверия к операционным системам снижаются и перемещаются на уровень ПК Фантом, который ввиду наличия исходных кодов небольшого объема можно полностью проанализировать

Преимущества ПК «ФАНТОМ»

- ❖ Существенным достоинством решения является возможность разворачивания ПК Фантом и рабочих мест на персональном переносимом USB-диске.
- ❖ При загрузке персонального компьютера с этого диска работа ПК Фантом и работа пользователя никак не отличаются от работы с встроенным диском компьютера. При этом внутренний диск полностью изолирован: вся информация хранится исключительно на внешнем диске пользователя, внутренний диск полностью защищен на чтение и запись информации

Функциональность

- ✓ Безопасная работа на персональном компьютере (коллективного пользования, домашний) в том числе с **индивидуального переносного USB-диска**;
- ✓ Одновременная изолированная работа заданного количества пользовательских систем с возможностью остановки процессов в неактивной системе;
- ✓ Контроль работы периферийных устройств компьютера, включая встроенную память и диск;
- ✓ Прозрачное функционирование для пользователя;
- ✓ Реализация криптографических функций на уровне гипервизора;
- ✓ Повышенная отказоустойчивость за счет механизма снимков состояния и хранилища резервных копий;
- ✓ Аудит происходящих событий;
- ✓ Контроль сетевого взаимодействия;
- ✓ Усиленная аутентификация пользователей.

«...Программное средство защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, и соответствует требованиям руководящего документа "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации" (Гостехкомиссия России, 1992) по 5 классу защищенности и технических условий ТУ 5011-001-17917145-2012 и может использоваться для защиты информации в автоматизированных системах до класса 1Г включительно...»

**СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**



**ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00**

**СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 2923**

Выдан 11 июля 2013 г.
Действителен до 11 июля 2016 г.

Настоящий сертификат удостоверяет, что программный комплекс «Фантом», разработанный и производимый ЗАО «РНТ» в соответствии с техническими условиями ТУ 5011-001-17917145-2012, функционирующий под управлением операционных систем, указанных в формуляре 30 5011-001-17917145-2012, является программным средством общего назначения со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, соответствует требованиям руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) - по 5 классу защищенности и технических условий при выполнении указаний по эксплуатации, приведенных в формуляре.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ОАО «Безопасность информационных технологий и компонентов» (аттестат аккредитации от 13.05.2003 № СЗИ RU.1190.В032.056) – техническое заключение от 16.05.2013, и экспертного заключения от 31.05.2013 органа по сертификации ЗАО «Научно-производственное объединение «Эшелон» (аттестат аккредитации от 02.12.2010 № СЗИ RU.2321.А101.013).

Заявитель: ЗАО «РНТ»
Адрес: 129515, г. Москва, 2-я Останкинская ул., д. 6
Телефон: (495) 777-7577

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям указанных в настоящем сертификате документов осуществляется испытательной лабораторией ООО «Центр безопасности информации».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ



А.Куп

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
11 июля 2013 г.

Развитие ПК Фантом

- ✓ Защита от скрытых каналов и уязвимостей аппаратного обеспечения
- ✓ Безопасное использование облачных средств хранения данных (частное облако, DropBox, SkyDrive, GitHub, Google Disk, Yandex Disk и др.)
- ✓ Защищенная обработка информации в соответствии требованиям регуляторов
- ✓ Безопасная удаленная работа с отдельными приложениями, сервисами на аппаратных единицах с установленной Системой
- ✓ Специализированные сервисы с функциональностью:
 - Антивирус
 - Маршрутизация и анализ трафика
 - Криптопровайдер
 - TLS-туннель с ГОСТ-шифрованием
 - Использование в ПКС-сетях



Варианты использования

- ✓ Работа одновременно в различных категорированных сегментах корпоративной сети
- ✓ Безопасное использование облачных средств хранения данных (**DropBox, SkyDrive, Google Disk, Yandex Disk** и др.)
- ✓ Гибкая интеграция с другими средствами защиты информации (антивирусы, СРД, межсетевые экраны, анализаторы уязвимостей и т.п.)
- ✓ Минимизация возможностей для векторов атак через переносимые устройства путём полного контроля подключаемых периферийных устройств
- ✓ Мониторинг информационного взаимодействия
- ✓ Повышенная отказоустойчивость и доступность

Примеры эксплуатации ПК ФАНТОМ

Применение ПК Фантом позволяет значительно упростить организационно-технические меры защиты информации, принимаемые в соответствии с российским законодательством и нормативными актами регуляторов:

- ✓ Работа персонала одновременно в различных категорированных сегментах корпоративной сети, например, работа трейдеров с торговыми площадками и одновременно в защищенном периметре локальной вычислительной сети
- ✓ Организация удаленного рабочего места сотрудников, например, из дома или в командировках
- ✓ Использование в системах дистанционного банковского обслуживания
- ✓ Организация шлюзов для работы с внешними по отношению к АБС системами: SWIFT, передачи данных в расчетный центр Банка России
- ✓ Защищенная передача информации между географически распределенными подразделениями многофилиальной организации



+7 (495) 777-7577

sales@rnt.ru