Информационная безопасность.
17 марта 2020
Программный комплекс
Абонентский облачный терминал

Писковский В.О.

Краткое описание

Абонентский облачный терминал (АОТ) - программное средство общего назначения с встроенными средствами защиты.

АОТ:

- ✓ **обеспечивает безопасную работу с конфиденциальной информацией**
- ✓ **устанавливается на персональном компьютере или ноутбуке**

СОСТАВНЫЕ ЧАСТИ:

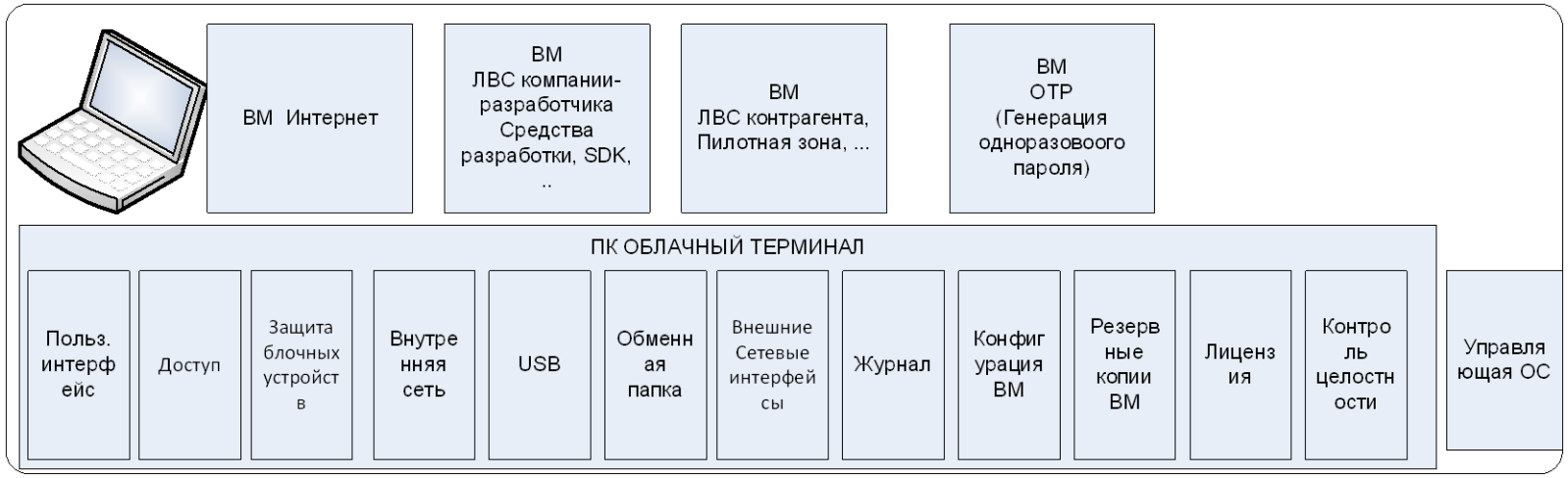
Управляющая ОС	Реализация работы сервисов и функций
ПК Абонентский облачный терминал	Конфигурирование и управление работой сервисов и функций: работа ВМ, доступ к периферии, защита блочных устройств, DHCP, NAT, VPN, FTP, политики безопасности, контроль целостности, антивирус, лицензирование, журналирование и анализ событий безопасности ...
Виртуальные машины (ВМ)	Выполнение сотрудником должностных обязанностей в изолированных предварительно настроенных автоматизированных рабочих местах, контролируемых ПК АОТ.

РАБОЧЕЕ МЕСТО С АОТ:

- → Защищённый удалённый доступ к серверам и услугам рабочей инфраструктуры, включая режим терминального доступа
- → Защищённый доступ к услугам ДМЗ
- → Работа эталонной ВМ с рабочей инфраструктурой
- → Работа эталонной ВМ ДМЗ с открытыми сетями
- → В случае режима VDI обеспечение непрерывности путём перемещения ВМ из рабочей инфраструктуры предприятия на персональный компьютер для работы off-line и обратно.
- → Защищённый юридически значимый документооборот с использованием облачной УКЭП
- → Безопасная одновременная работа во всех перечисленных выше режимах

Состав

Гипервизор полностью контролирует функционирование гостевых ОС, периферийные устройства компьютера и сетевое взаимодействие. Таким образом требования доверия к ОС снижаются и перемещаются на уровень гипервизора, который ввиду наличия относительно небольшого объёма исходных кодов и ограниченной функциональности легче проанализировать.



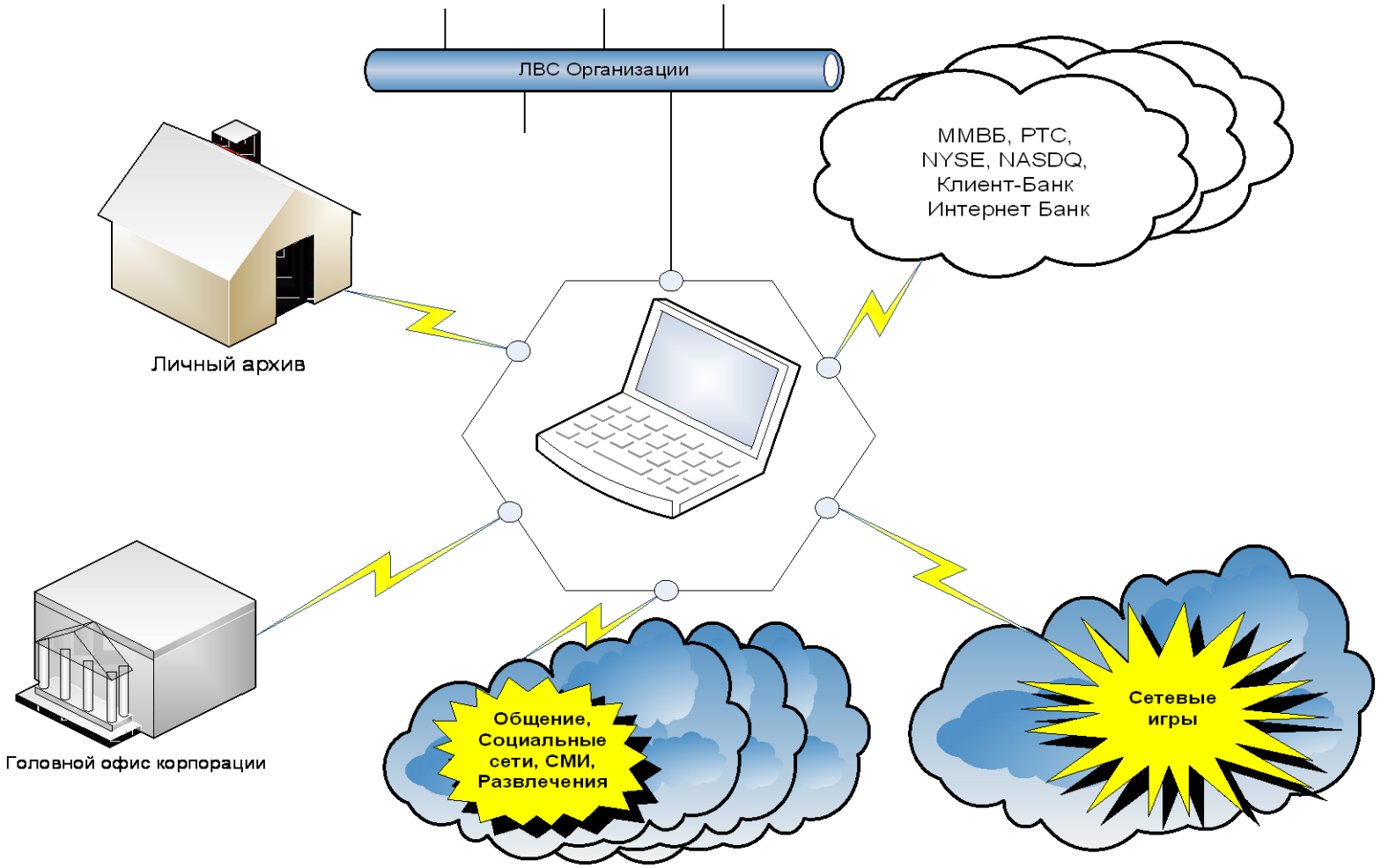
Функциональность

- ✓ Защищённый от внесения несанкционированных изменений режим функционирования рабочего места
- ✓ Загрузка с неизменяемого(опционально) образа ВМ
- ✓ Возможность работы в автономном режиме для оптимизации загрузки каналов
- ✓ Изоляция рабочих мест, работа в нескольких изолированных контурах, сегментах сети
- ✓ Удалённое администрирование, включая управление правами доступа пользователей к информационным ресурсам
- ✓ Общий ресурс управляемого обмена информацией между ВМ с антивирусом
- ✓ Хранение данных пользователя в зашифрованном виде непосредственно на персональном компьютере или ноутбуке
- ✓ Мониторинг действий пользователя по передаче информации между рабочими средами
- ✓ Интеграция со средствами многофакторной авторизации
- ✓ Защита от НСД с использованием российских СКЗИ
- ✓ Идентификация рабочего места, оснащенного АОТ, по фотографии документа, отображаемого на его экране

Ключевые возможности

- ✓ До 8 одновременно запущенных виртуальных машин (ВМ) с настраиваемой специализацией
- ✓ Контроль целостности данных – ВМ возвращается в исходное состояние при выключении
- ✓ Списки доверенных носителей информации
- ✓ Защита от НСД системных и пользовательских данных
- ✓ Использование встроенного межсетевого экрана
- ✓ Многофакторная аутентификация с подтверждением одноразовым паролем
- ✓ Запуск с любого, в том числе отчуждаемого носителя
- ✓ Гибкая настройка под нужды и потребности клиентов
- ✓ Не требует специального обучения – в ВМ используются знакомые пользователям операционные системы и рабочие окружения
- ✓ Безопасное соединение (VPN) с удаленными серверами или облачными сервисами

Варианты использования



Использование на предприятии, в компании

В практической деятельности по управлению системой безопасности и ИТ-системой предприятия наиболее ответственными, трудоёмкими и продолжительными задачами являются:

- → Управление Конфигурациями
- → Управление Изменениями
- → Управление Релизами

Предлагаемое решение позволяет значительно сократить трудоемкость и риски, возникающие в этих процессах

СОСТАВНЫЕ ЧАСТИ:

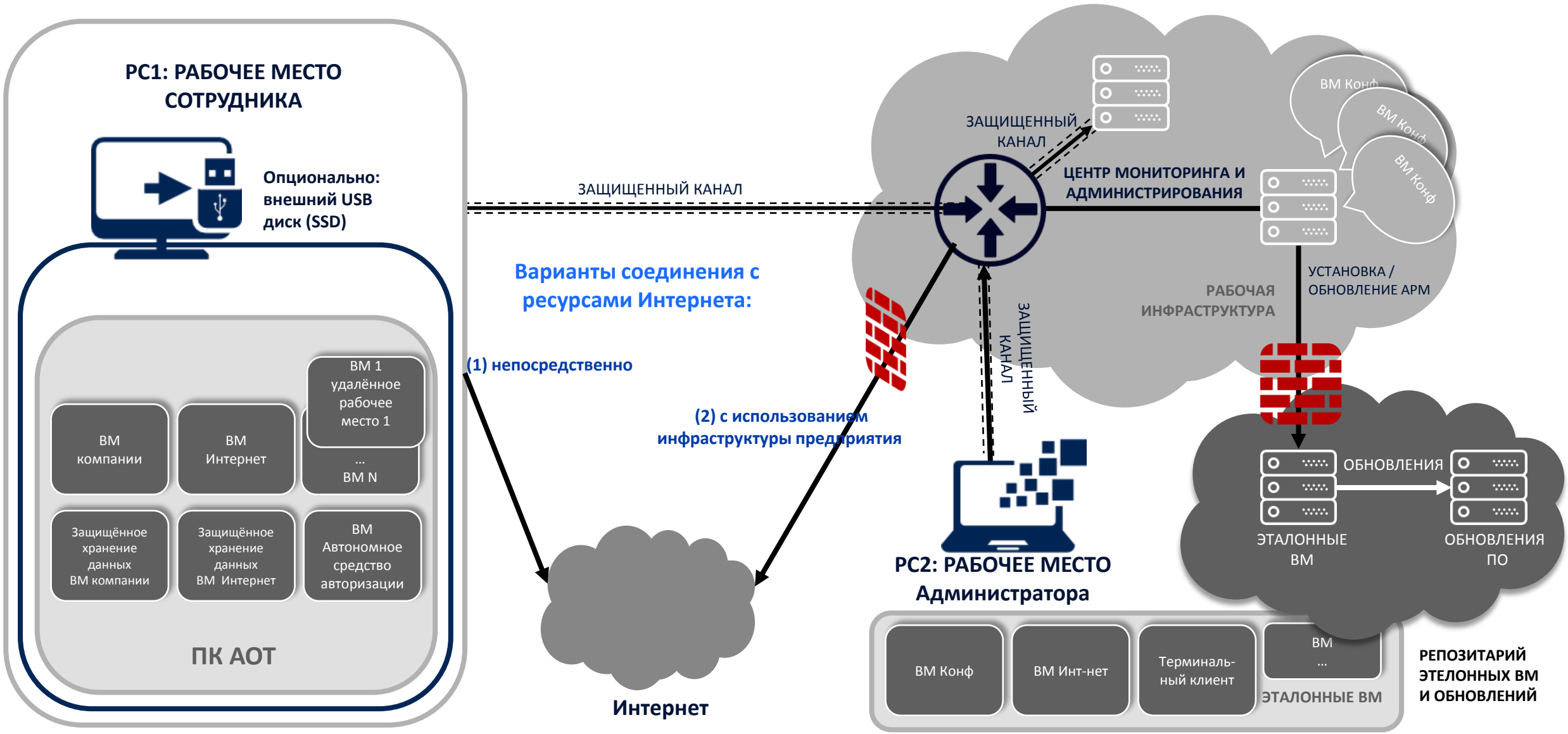
Эталонные ВМ, серверы с обновлениями ПО.

РЕПОЗИТАРИЙ ЭТАЛОННЫХ ВМ И ОБНОВЛЕНИЙ	Формирование, администрирование и хранение проверенных, согласованных, безопасных эталонных конфигураций ВМ осуществляется централизованно, что снижает трудоемкость и риски.
РАБОЧАЯ ИНФРАСТРУКТУРА ПРЕДПРИЯТИЯ	В продукционном ландшафте информационной инфраструктуры находятся серверы, сетевые и иные компоненты, ПО в постоянной (промышленной) эксплуатации. Решение исключает необходимость администрирования ОС и систем безопасности на рабочих местах
ДЕМИЛИТАРИЗОВАННАЯ ЗОНА	Сервисы для работы с открытыми сетями. Задача – обеспечение безопасного взаимодействия с открытыми сетями.

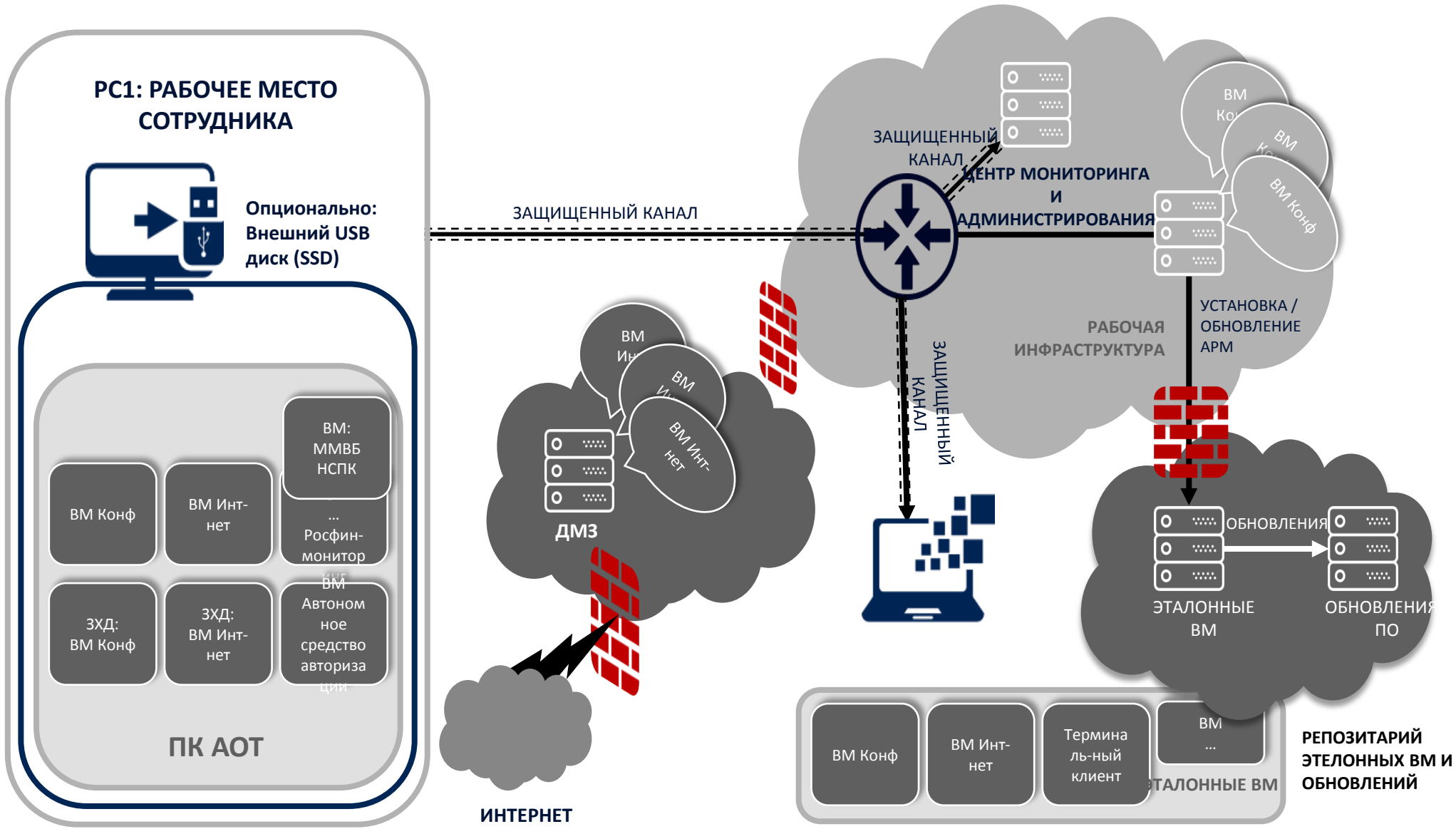
РАБОЧЕЕ МЕСТО С ПК «АОТ»:

- → Защищённый доступ к серверам и услугам рабочей инфраструктуры
- → Защищённый доступ к услугам ДМЗ
- → Работа эталонной ВМ с рабочей инфраструктурой
- → Работа эталонной ВМ ДМЗ с открытыми сетями
- → В случае режима VDI обеспечение непрерывности путём перемещения ВМ из рабочей инфраструктуры предприятия на персональный компьютер для работы off-line и обратно.
- → Защищённый юридически значимый документооборот с использованием облачной УКЭП
- → Безопасная одновременная работа во всех перечисленных выше режимах

Принципиальная схема решения. 1



Принципиальная схема решения. 2



Реализация на внешнем носителе

АОТ может быть использован:

- ✓ Локально в офисе, для обеспечения безопасности конечных АРМ в многоуровневой системе защиты информации
- ✓ В поездках, для установления безопасного соединения с корпоративными серверами или облачными приложениями

Целевые секторы рынка:

- ➢ B2B: финансовый, нефтяной, газовый
- ➢ B2G: Государственные учреждения

Функционирование при реализации на внешнем носителе

Альтернативная загрузка компьютера с использованием АОТ

Подключение внешнего носителя информации, содержащего АОТ

Настройка параметров: соединение, пользователи, доверяемые носители информации и т.д.

Запуск виртуальной машины и установка безопасного соединения

Система идентификации рабочего места, оснащённого АОТ, по фотографии документа, отображаемого на экране

Схема решения

РАБОЧЕЕ МЕСТО СОТРУДНИКА

Встраивание цифровых водяных знаков (ЦВЗ) в изображение

Службы обеспечения ПК АОТ

ВМ Конф.

DHCP

Средства защиты ПК

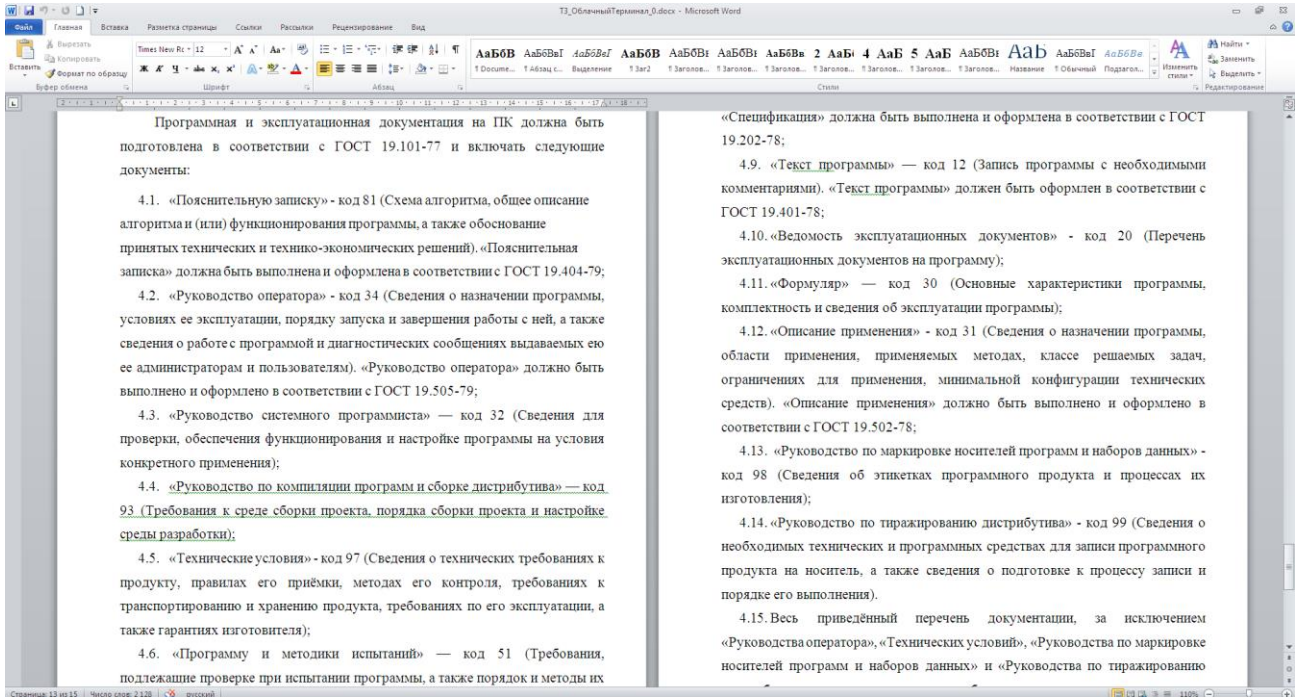
ЗХД

FTP

ПК АОТ

Функциональные требования

ЦВЗ незаметен



Программная и эксплуатационная документация на ПК должна быть подготовлена в соответствии с ГОСТ 19.101-77 и включать следующие документы:

4.1. «Пояснительную записку» - код 81 (Схема алгоритма, общее описание алгоритма и (или) функционирования программы, а также обоснование принятых технических и технико-экономических решений). «Пояснительная записка» должна быть выполнена и оформлена в соответствии с ГОСТ 19.404-79;

4.2. «Руководство оператора» - код 34 (Сведения о назначении программы, условиях ее эксплуатации, порядку запуска и завершения работы с ней, а также сведения о работе с программой и диагностических сообщениях выдаваемых ею ее администраторам и пользователям). «Руководство оператора» должно быть выполнено и оформлено в соответствии с ГОСТ 19.505-79;

4.3. «Руководство системного программиста» — код 32 (Сведения для проверки, обеспечения функционирования и настройке программы на условия конкретного применения);

4.4. «Руководство по компиляции программ и сборке дистрибутива» — код 93 (Требования к среде сборки проекта, порядка сборки проекта и настройке среды разработки);

4.5. «Технические условия» - код 97 (Сведения о технических требованиях к продукту, правилах его приёмки, методах его контроля, требованиях к транспортированию и хранению продукта, требованиях по его эксплуатации, а также гарантиях изготовителя);

4.6. «Программу и методики испытаний» — код 51 (Требования, подлежащие проверке при испытании программы, а также порядок и методы их

«Спецификация» должна быть выполнена и оформлена в соответствии с ГОСТ 19.202-78;

4.9. «Текст программы» — код 12 (Запись программы с необходимыми комментариями). «Текст программы» должен быть оформлен в соответствии с ГОСТ 19.401-78;

4.10. «Ведомость эксплуатационных документов» - код 20 (Перечень эксплуатационных документов на программу);

4.11. «Формуляр» — код 30 (Основные характеристики программы, комплектность и сведения об эксплуатации программы);

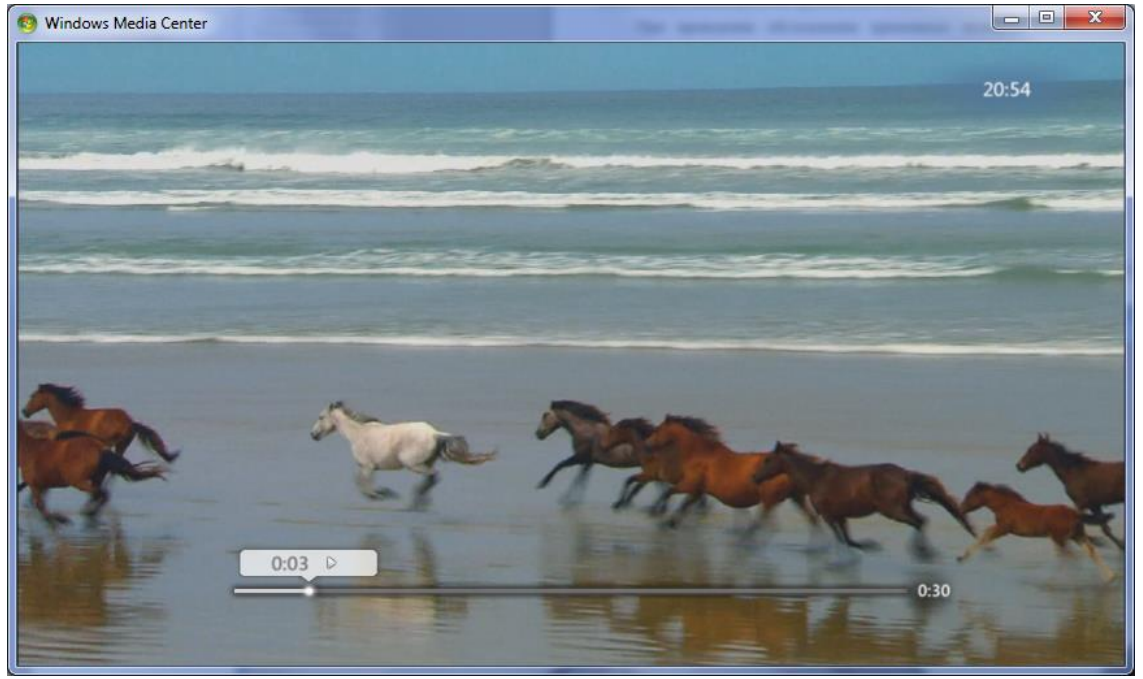
4.12. «Описание применения» - код 31 (Сведения о назначении программы, области применения, применяемых методах, классе решаемых задач, ограничениях для применения, минимальной конфигурации технических средств). «Описание применения» должно быть выполнено и оформлено в соответствии с ГОСТ 19.502-78;

4.13. «Руководство по маркировке носителей программ и наборов данных» - код 98 (Сведения об этикетках программного продукта и процессах их изготовления);

4.14. «Руководство по тиражированию дистрибутива» - код 99 (Сведения о необходимых технических и программных средствах для записи программного продукта на носитель, а также сведения о подготовке к процессу записи и порядке его выполнения).

4.15. Весь приведённый перечень документации, за исключением «Руководства оператора», «Технических условий», «Руководства по маркировке носителей программ и наборов данных» и «Руководства по тиражированию

ЦВЗ не влияет на работу ОС и пользователя



Технические требования

- ЦВЗ содержит идентификатор рабочего места
- Идентификатором является строка, например: 130A-F7C5-712B-88A7
- Количество вариантов в зависимости от длины идентификатора:

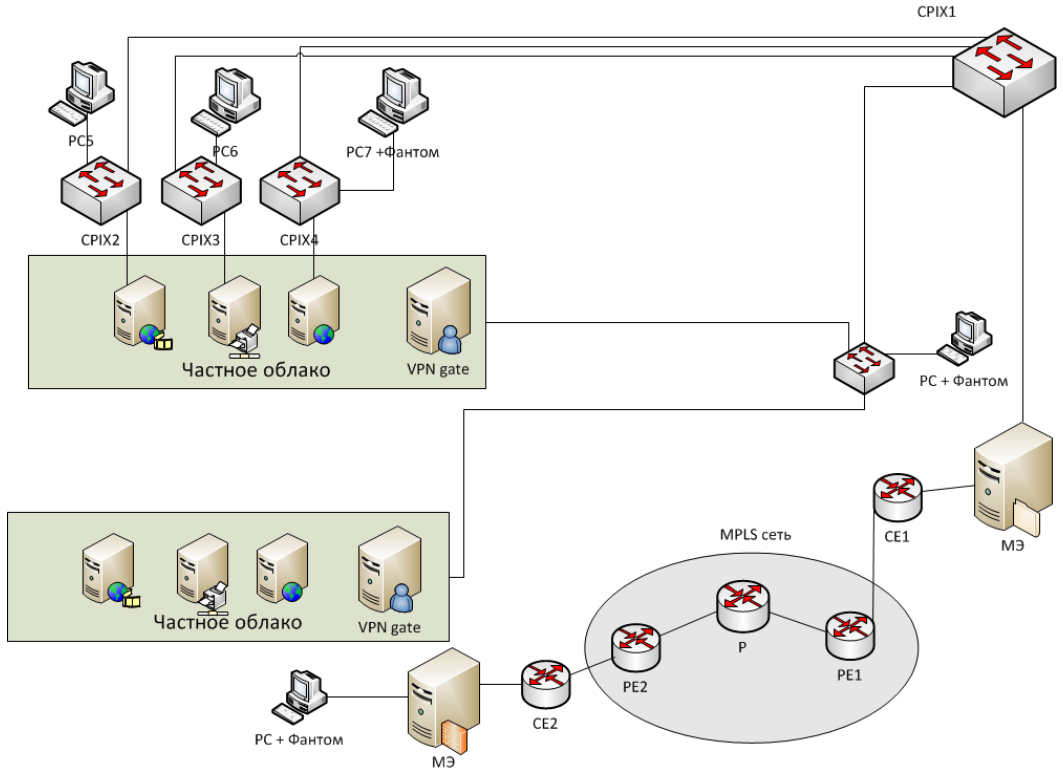
Количество вариантов	
Биты	**Вариантов**
64	1,8E+19
32	4,3E+09
16	6,6E+04
8	2,6E+02

- Идентификатор однозначно определяется при помощи специального ПО, разработанного для обработки фотографии документа, например, на мобильном телефоне
- … другие требования

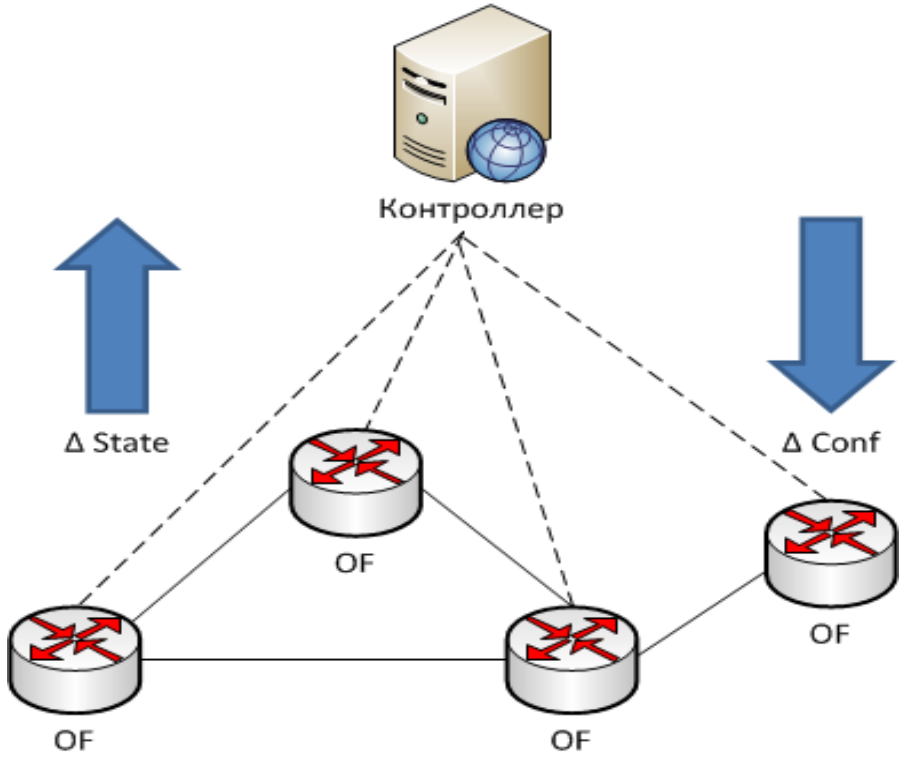
Информационная безопасность. Реконфигурация ПКС

Традиционная сеть и ПКС

Традиционная сеть



Программно-конфигурируемая сеть



Внесение изменений в продукционную ИТ-инфраструктуру предприятия

Традиционная сеть

- Длительное документальное согласование схем коммутации
- «Ручная» конфигурация сети, потоков, сетевых устройств на основе документально согласованных схем

Программно-конфигурируемая сеть

- Наличие предварительно разработанных и отлаженных приложений управления сетью передачи данных
- Автоматизированная конфигурация сети контроллером на основе пользовательских запросов при помощи указанных приложений управления сетью в соответствии с принятыми политиками безопасности

Конфликты конфигурации

Традиционная сеть

- Разрешаются «вручную» на этапе документального согласования схем коммутации и опытно-промышленной эксплуатации внедряемого сервиса
- Изменения конфигурации единичные и всегда авторизованы ответственным сотрудником

Программно-конфигурируемая сеть

- Будучи замеченными, требуют внесения изменений в приложения, управляющими сетью, конфигурационные данные приложений
- Изменения конфигурации вызваны частыми конкурирующими запросами пользователей или сетевых сервисов. Приходится полагаться на корректность работы приложения

Методы минимизации рисков возникновения конфликтов

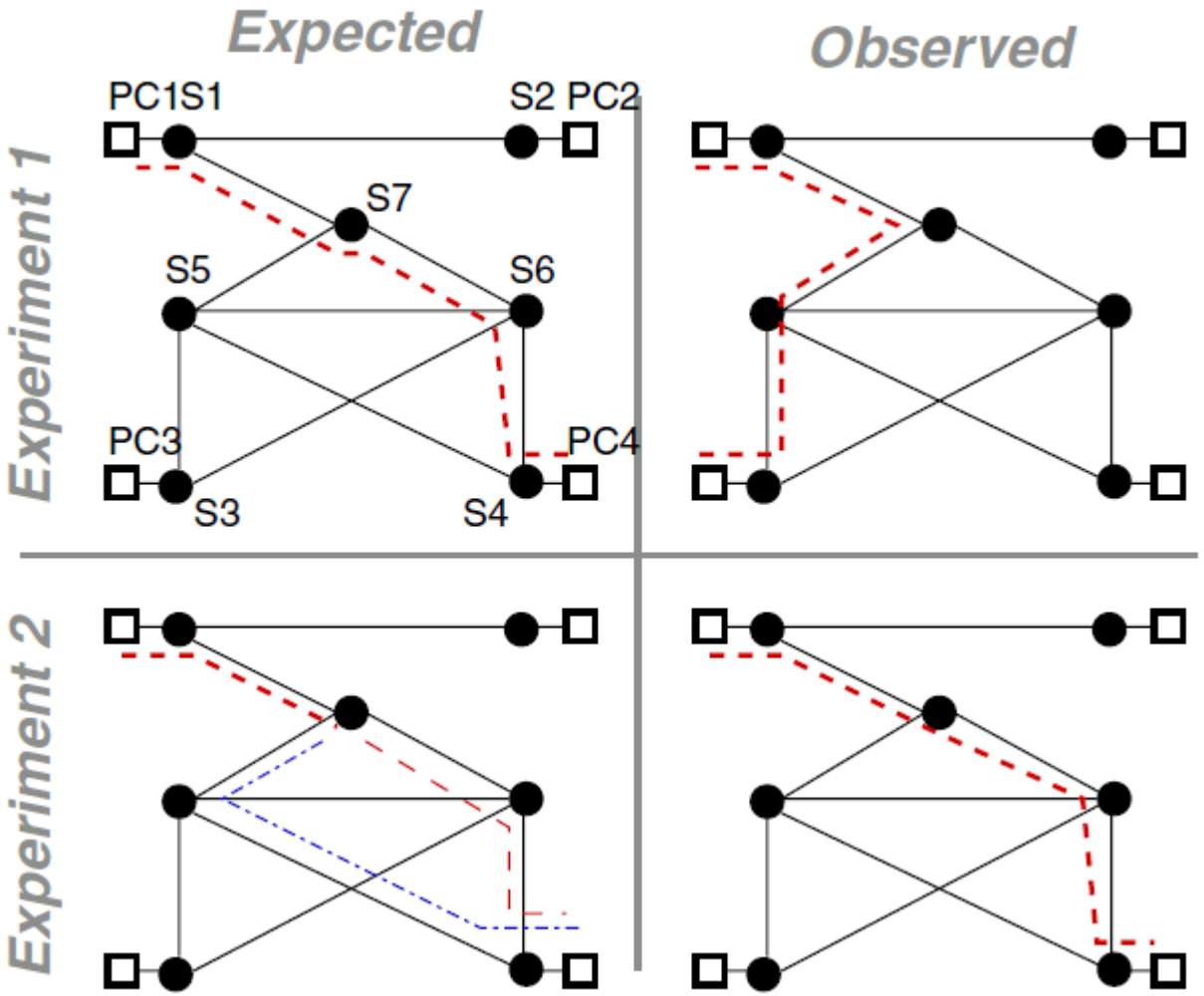
Традиционная сеть

- Экспертный анализ, внесение изменений в документально согласованные схемы, повторное согласование документов
- Внесение «вручную» изменений в конфигурацию
- Последующий экспертный контроль эксплуатации сети

Программно-конфигурируемая сеть

- Теоретическое обоснование методов и алгоритмов, по которым работают названные приложения.
- Внесение изменений в приложения
- Экспертный контроль эксплуатации сети

Пример конфликтующих приложений



Конфликт вызван порядком выполнения приложений контроллера

Источник:
A General Approach to Conflict Detection in Software-Defined Networks
Cuong Ngoc Tran,· Vitalian Danciu
Received: 22 April 2019
/ Accepted: 24 June 2019

Предлагаемый подход

Разработка математического аппарата для теоретического обоснования методов и алгоритмов, используемых при проектировании приложений, управляющих программно-конфигурируемой сетью, с целью минимизации рисков возникновения конфликтов и их последствий