kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Secure Hypervisor

Решение «Лаборатории Касперского» для обеспечения безопасности АСУ ТП

АСУ ТП как сложная комплексная система

Современные системы промышленной автоматизации (АСУ ТП) очень сложны и должны соответствовать широкому набору требований: выполнять множество функций, обладать высокой доступностью, включать индикаторы безопасности, поддерживать работу с географически распределенной промышленной инфраструктурой, оперировать в условиях жесткого реального времени и соответствовать требованиям отраслевого законодательства. При этом реально работающие АСУ ТП часто представляют собой сложное сочетание технологий, стандартов и протоколов, которые могут быть частично устаревшими, более не поддерживаемыми, небезопасными или оставшимися по наследству от предыдущих версий ПО.

Как показывает многолетний опыт «Лаборатории Касперского», угрозы кибербезопасности АСУ ТП часто недооцениваются. В качестве иллюстрации можно привести следующие распространённые представления:

Распространённое представление	В действительности
АСУ ТП используют проприетарные стандарты и протоколы, о которых знают только эксперты, и эта информация недоступна для хакеров.	Документация АСУ ТП, спецификации протоколов и т.д. доступны в интернете, включая описания уязвимостей и практические руководства по взлому.
АСУ ТП функционируют в закрытой среде.	Многие сети АСУ ТП прямо или косвенно подключены к общедоступным сетям, и сервисы АСУ ТП могут стать мишенью для удаленной атаки злоумышленников.
АСУ ТП не могут быть атакованы внутренними нарушителями.	С АСУ ТП работает много людей. Нельзя гарантировать, что среди них нет злоумышленников. Кроме того, добросовестные сотрудники могут невольно или неосознанно способствовать проведению атаки (проблема confused deputy).
Использование современных технологий позволяет избежать рисков.	АСУ ТП имеют долгий срок службы, на протяжении которого трудно поддерживать их в актуальном по отношению к новым угрозам состоянии. За время эксплуатации технологии могут устареть.

Аспекты кибербезопасности
Управление организацией
Технологии
Человеческий фактор
Текущее и сервисное обслуживание
Внешнее и внутреннее окружение

Требования IT-безопасности	Требования безопасности АСУ ТП
Конфиденциальность Целостность Доступность	Доступность Целостность Конфиденциальность Функциональная безопасность Окружение Внешние зависимости Нормы законодательства и отраслевые стандарты Многое другое

Примеры атак
Атака с использованием переполнения буфера
Внедрение кода
Атака при отсутствии проверки вводимых данных
Атаки при наличии физического доступа к оборудованию
Взлом учётных записей
Атаки, эксплуатирующие слабые механизмы аутентификации
Ошибки в алгоритмах шифрования
Манипуляции с путями в файловой системе
Заражение вредоносным кодом при загрузке веб-страниц
Подделка межсайтовых запросов
Атаки, направленные на исчерпание ресурсов/отказ в обслуживании

Атаки на АСУ ТП могут преследовать различные цели. Например, известны попытки вызвать сбои в работе индустриальных систем с целью получения конкурентного преимущества или финансовой выгоды в форме выкупа. Имеются примеры террористических актов в форме атак на АСУ ТП. В ряде случаев атаки проводятся из хулиганских побуждений.

Подобные атаки возможны благодаря наличию уязвимостей, появившихся из-за просчетов на этапе проектирования АСУ ТП, ошибок в реализации ПО, целенаправленно внедренных закладок, а также нарушений, допущенных в процессе эксплуатации систем.

«Лаборатория Касперского» предлагает технологии, которые позволяют значительно повысить уровень безопасности промышленных решений с учётом обширного опыта, накопленного в области разработки и эксплуатации АСУ ТП.

Источники угроз и проблем

Кибербезопасность АСУ ТП требует целостного всестороннего подхода на основе тщательного анализа множества факторов, включая:

1. Общее управление организацией:
- Зачастую кибербезопасность не входит в список приоритетных бизнес-целей организации;
- АСУ ТП часто не считаются частью IT-инфраструктуры и обслуживаются по упрощённым процедурам;
- Сотрудники организации могут не обладать достаточными знаниями и квалификацией;
- Вопросы амортизации и закупок рассматриваются отдельно от вопросов кибербезопасности.

2. Технологические аспекты:
- Использование устаревших технологий;
- Проектирование АСУ ТП без учёта соображений ИБ;
- Использование небезопасных, уязвимых для атак протоколов;
- Ошибочные представления об операционном окружении;
- Вопросы, связанные с удалённым доступом.

3. Человеческий фактор:
- Проблемы в связи с отсутствием чётко описанных политик и процедур;
- Возможные атаки со стороны недобросовестных сотрудников (действующих и бывших);
- Возможность невольного или неосознанного участия добросовестных сотрудников в атаке.

4. Текущее и сервисное обслуживание:
- Вопросы управления учётными записями;
- Отсутствие чётких процедур управления изменениями и анализа их последствий с точки зрения ИБ;
- Наличие администраторов с правами суперпользователя;
- Возможные проблемы, связанные с установкой обновлений;
- Вопросы защиты от вредоносного ПО;
- Возможности доступа к аппаратным средствам и сетевым ресурсам.

5. Внешнее и внутреннее окружение:
- Вопросы физической безопасности;
- Внешние зависимости АСУ ТП (энергоснабжение, IT-инфраструктура)
- Возможность доступа к объектам АСУ ТП лиц, не являющихся сотрудниками организации, удалённый доступ.

Для определённых групп киберпреступников АСУ ТП представляют привлекательную мишень. Причин этому множество; мы назовём лишь две из них. Во-первых, атака на такой объект может привести к катастрофическим последствиям как для отдельных лиц и организаций, так и для окружающей среды и даже общества в целом. Во-вторых, у этих объектов, как правило, большая поверхность атаки – АСУ ТП используют множество технологий, значительная часть которых бывает недостаточно защищена.

Обеспечение кибербезопасности АСУ ТП с помощью Kaspersky Secure Hypervisor

Наряду с обширным списком решений для обеспечения кибербезопасности крупного бизнеса и домашних пользователей, «Лаборатория Касперского» предлагает специализированные продукты: KasperskyOS, Kaspersky Security System (KSS) и Kaspersky Secure Hypervisor (KSH). Их ключевой особенностью является инновационный подход, который позволяет разделить систему на изолированные домены безопасности и контролировать все взаимодействия между ними в соответствии с заданными политиками безопасности.

Kaspersky Secure Hypervisor (KSH) – это гипервизор второго типа, который работает поверх микроядра KasperskyOS. Основное преимущество использования виртуализации состоит в отделении потенциально ненадёжных гостевых операционных систем друг от друга и от критических сервисов, размещённых на той же физической машине. Это позволяет сократить поверхность атаки и свести к минимуму возможные последствия эксплуатации уязвимостей. Гипервизор защищён от гостевой ОС таким образом, что её вредоносные действия не могут причинить вред критическим службам или самому гипервизору. Дополнительным преимуществом использования KSH является сокращение расходов на обслуживание аппаратного обеспечения.

«Лаборатория Касперского» рекомендует Kaspersky Secure Hypervisor для обеспечения безопасности АСУ ТП. При использовании гипервизора многие проблемы с безопасностью могут быть решены без каких-либо модификаций действующего ПО АСУ ТП. Возможности, предоставляемые KSH, дают существенные преимущества при разработке новых решений для обеспечения безопасности АСУ ТП.

Практические примеры защиты АСУ ТП с помощью KSH:

1. Контроль периферии

KSH обеспечивает полную изоляцию гостевых операционных систем, что позволяет предоставлять или не предоставлять доступ к периферийным устройствам. В частности, KSH может:

- Деактивировать неиспользуемые устройства (USB, Bluetooth, Wi-Fi, камеры, микрофоны) для сокращения поверхности атаки.
- Контролировать доступ к периферийным устройствам в соответствии с заданными политиками безопасности (совместно с KSS).
- Осуществлять авторизацию доступа к устройствам.

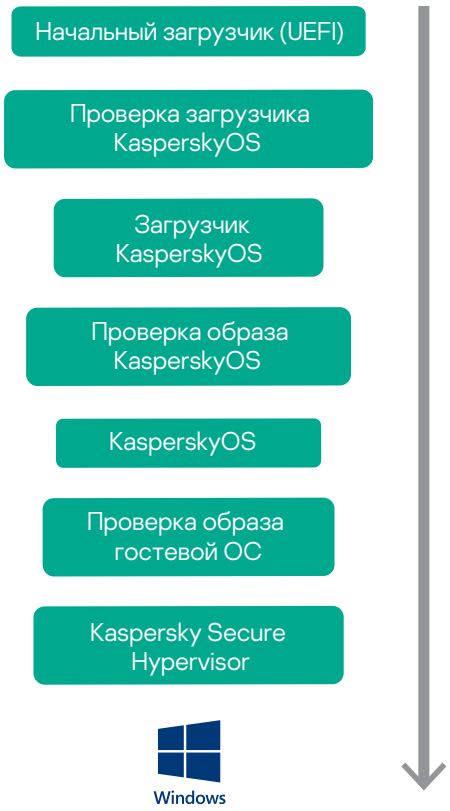
2. Безопасное обновление

По статистике, часть вредоносного ПО попадает в систему во время её обновления. KSH предоставляет надёжные инструменты безопасного обновления ПО АСУ ТП. Для этого средствами KSH реализуется независимый канал доставки обновлений. Проверка их целостности и аутентичности выполняется с помощью доверенных механизмов, работающих на уровне KasperskyOS. Гостевая ОС не может повлиять на этот процесс.

3. Доверенная аутентификация

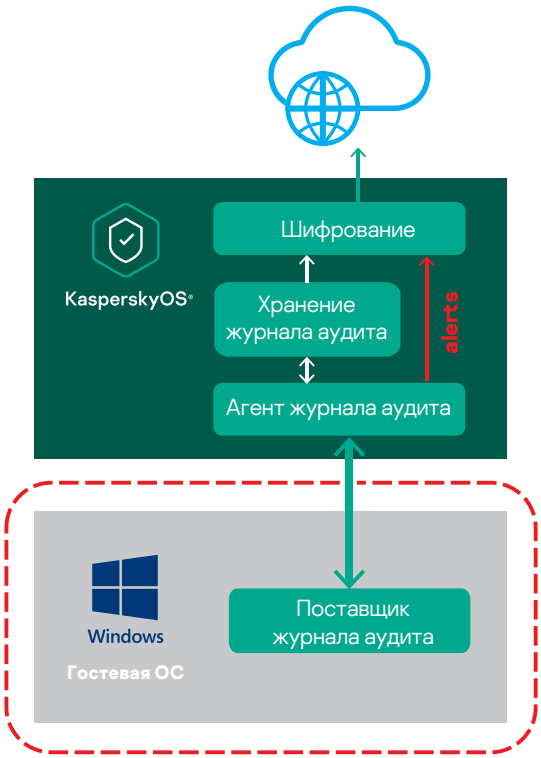
Гостевые ОС сложны и часто содержат уязвимости, поэтому их системы аутентификации нельзя считать надёжными. Так как KSH работает в доверенном окружении, есть возможность обеспечить дополнительные, независимые, надёжные и безопасные механизмы аутентификации на уровне KasperskyOS. При использовании KSH доступ к гостевой ОС предоставляется лишь в том случае, если пользователь прошел аутентификацию на уровне KasperskyOS.

Дополнительным преимуществом такого подхода является возможность реализовать механизмы аутентификации, не поддерживаемые гостевой ОС (т.е. с помощью не только пароля, но и токена, смарт-карты, по отпечатку пальца и др.).



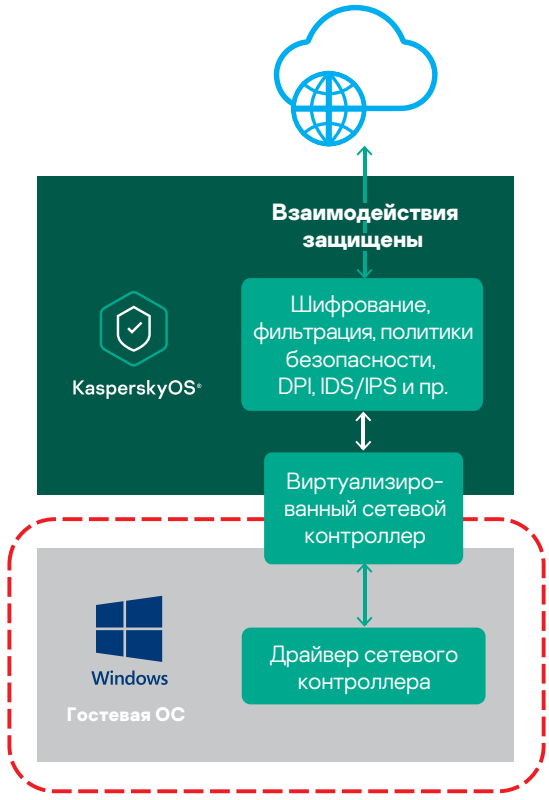
4. Безопасная загрузка

Средствами KSH можно реализовать безопасную загрузку гостевой ОС – одну из ключевых мер безопасности для встраиваемых систем. Она включает набор процедур верификации, основанных на аппаратных механизмах защиты. Безопасная загрузка обеспечивает целостность и аутентичность образа ОС (ядра ОС и файловых систем) и его загрузчиков, а также гарантирует, что в случае повреждения или модификации гостевая ОС не будет загружена.



5. Безопасный аудит

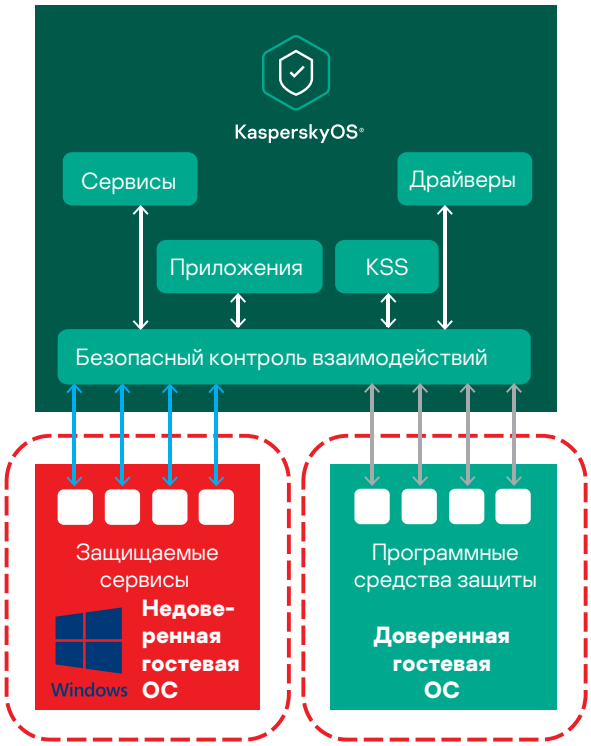
Использование KSH позволяет решить проблему подмены записей в журнале событий гостевой ОС. Для этой цели между гостевой ОС и KSH организуется канал для передачи записей, которые безопасно сохраняются на стороне KSH, после чего гостевая ОС не может получить к ним доступ. В KSH также реализован набор дополнительных механизмов для защиты полученных записей. Так, использование подхода на базе блокчейн позволяет гарантировать защиту записей от подмены или модификации даже в случае физического доступа к устройству, а с помощью современных алгоритмов шифрования можно надёжно защитить данные при их передаче в удалённые компоненты системы.



6. Защита распределённых систем

Распределённые системы АСУ ТП зачастую весьма сложны и имеют неоднородную структуру, а их поддержка затрудняется отсутствием единой точки администрирования. Они могут иметь уязвимости, которые чрезвычайно сложно обнаружить, или использовать устаревшие уязвимые протоколы (например, SSL v3.0). Модернизация подобных систем является сложной и затратной задачей. Во многих случаях владельцы уделяют больше внимания доступности АСУ ТП в ущерб её безопасности, что делает систему уязвимой.

Средствами KSH можно организовать зашифрованный доверенный канал для информационного обмена в рамках распределённой АСУ ТП. Гостевая ОС видит этот канал как простой сетевой адаптер и продолжает отправлять данные без необходимости принятия дополнительных мер по их защите. KSH получает незащищённый пакет, зашифровывает его, преобразует в соответствии с требованиями протокола передачи данных, организуя таким образом изолированную защищённую сеть, в которой невозможно перехватить или подменить какие-либо данные.



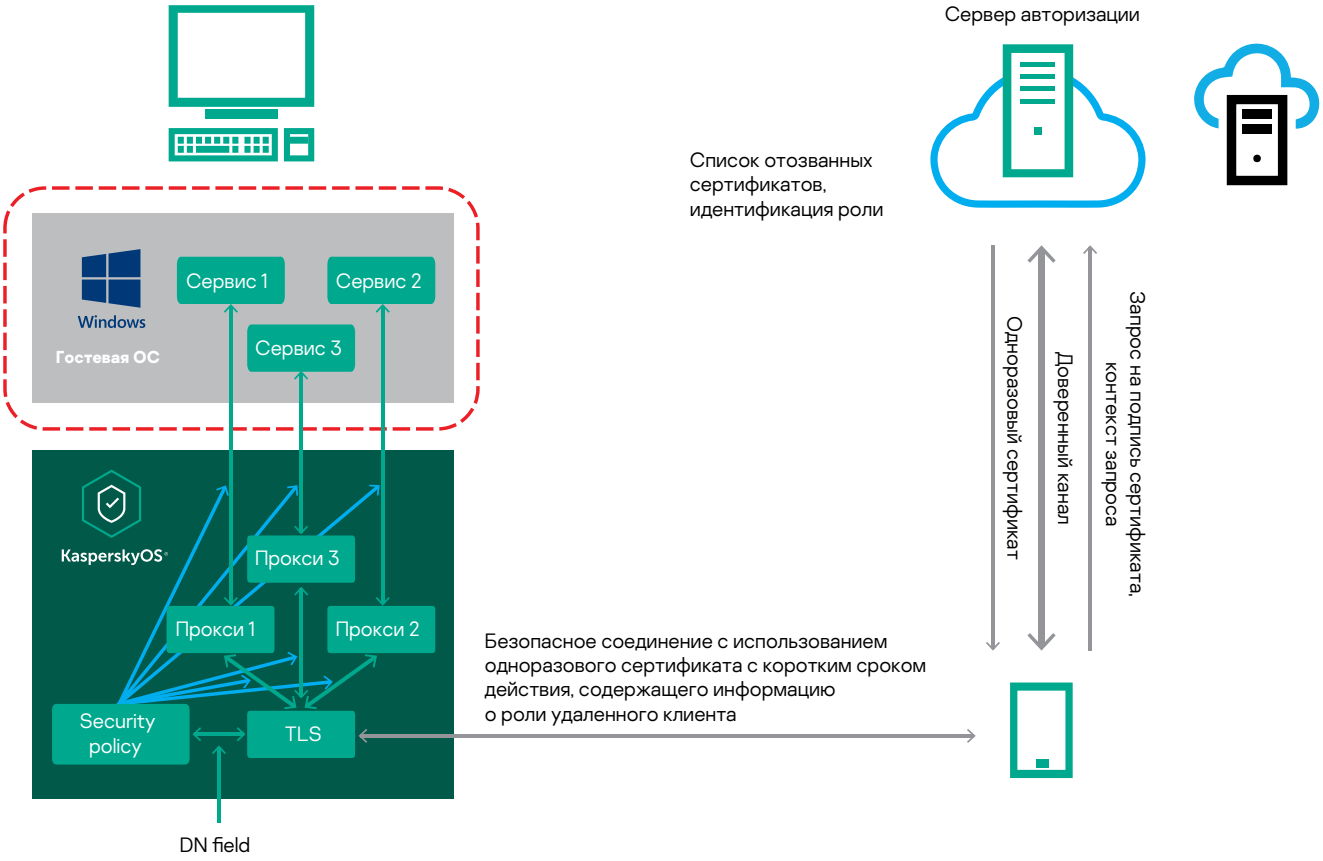
7. Дополнительная доверенная гостевая ОС

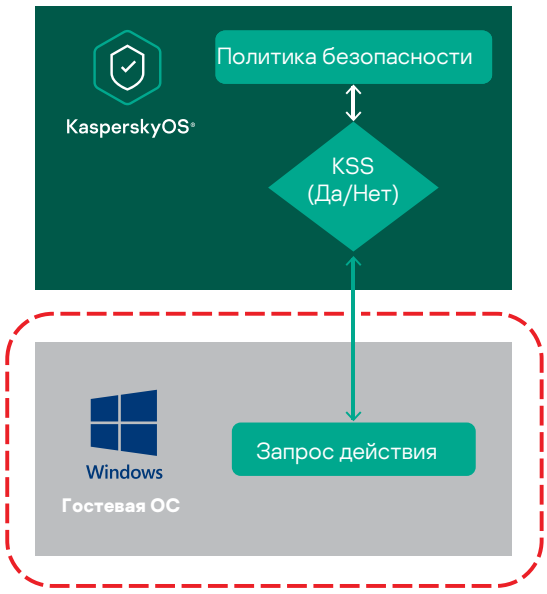
Если непосредственное внедрение технологий и продуктов для создания полностью безопасной инфраструктуры АСУ ТП представляется слишком сложным, затратным или нецелесообразным, KSH позволяет задействовать для решения задач безопасности дополнительную доверенную гостевую ОС, в том числе на базе Linux (конечно, в этом случае потребуются соответствующие ограничительные меры). В доверенной гостевой ОС может быть установлен набор готовых, не требующих доработки приложений и сервисов, например ПО, реализующее различные криптографические протоколы, DPI, инструменты администрирования и т.д. KSH обеспечивает безопасную коммуникацию между доверенной и недоверенной ОС. Общая защищённость решения при этом существенно возрастает благодаря возможности контролировать работу доверенной ОС на всех этапах её функционирования, что позволяет максимально сократить поверхность атаки доверенной гостевой ОС.

8. Доступ на основе ролей и полномочий

Пользователи АСУ ТП обладают различными полномочиями. При этом система безопасности на базе ролевого доступа, реализуемая в ОС общего назначения, не может считаться надёжной, поскольку сведения о ролях и полномочиях пользователей определяются самой ОС. Чтобы сделать этот процесс доверенным, функция контроля ролей и полномочий может быть передана KSH, который будет определять атрибуты пользователей с помощью собственных доверенных инструментов. Затем информация о ролях и полномочиях пользователей передаётся в готовом виде в гостевую ОС, и она не может повлиять на этот вердикт. Применение описанного подхода позволяет избежать многих ошибок при организации ролевого доступа.

Кроме того, есть возможность установить на стороне KasperskyOS различные прокси-сервисы, отвечающие за коммуникацию с определёнными службами гостевой ОС. Средствами Kaspersky Security System на общесистемном уровне для прокси-сервисов задаются необходимые политики безопасности, описывающие в том числе вопросы взаимодействия с сервисами гостевой ОС. Если гостевая ОС каким-либо образом нарушит эти политики при работе с прокси-сервисами, такая попытка будет немедленно обнаружена и нейтрализована.





9. Авторизация действий приложений гостевой ОС

KSH предоставляет инструменты для управления работой приложений гостевой ОС в соответствии с политиками безопасности, заданными для решения в целом. Как правило, гостевую ОС можно рассматривать как достаточно доверенную для работы приложений АСУ ТП, но при этом действия, выполняемые АСУ ТП, могут потребовать дополнительного контроля, так как вследствие возможных ошибок в программном коде, недочётов, допущенных при проектировании системы, или необдуманных действий пользователя АСУ ТП может выполнить опасную или недопустимую операцию. Чтобы исключить подобные ситуации, KSH предоставляет интерфейс, позволяющий приложению гостевой ОС дополнительно запросить разрешение на выполнение тех или иных действий. Через этот интерфейс приложение гостевой ОС может обратиться напрямую к Kaspersky Security System, а KSS на основе политики безопасности, заданной для решения в целом, вычислит вердикт о возможности/невозможности операции и вернёт его приложению. После чего, в случае отрицательного вердикта, приложение заблокирует выполнение операции.

Таким образом, у приложений гостевой ОС появляется независимый механизм, позволяющий контролировать соответствие выполняемых операций общей политике безопасности решения.

10. Другие возможности

Кроме описанных выше, KSH предоставляет ряд других инструментов, позволяющих существенно повысить уровень защищённости решений АСУ ТП. Средствами KSH можно реализовать Trusted Execution Environment (TEE) для гостевых ОС, что даёт возможность вынести критические с точки зрения безопасности функции (например, шифрование, хранение важных данных, таких как сертификаты и ключи, и т.д.) за пределы гостевой ОС – в безопасное окружение, функционирующее на уровне KasperskyOS.

При использовании сервисов безопасности KSH появляется возможность контролировать доступ гостевых ОС к системным ресурсам (например, к памяти или периферии).

Сервисы KSH позволяют обеспечить мониторинг состояния гостевой ОС (сбор статистики об использовании памяти, процессорного времени, сведений о работе аппаратуры), реализовать независимый механизм перезапуска гостевой ОС в случае обнаружения зависаний, а также формировать оповещения о высокой загрузке и исчерпании ресурсов.

Кроме того, может быть реализован набор вспомогательных сервисов, таких как управление работой гостевой ОС на системном уровне с использованием единой для решения политики безопасности, прозрачное для гостевой ОС резервное копирование и восстановление данных и др.

PcVue Solutions
Your Independent Global SCADA Provider

Совместные проекты

Kaspersky Secure Hypervisor является новым продуктом на рынке. В настоящее время «Лаборатория Касперского» реализует совместный проект с компанией ARC Informatique – ведущим европейским производителем ПО для промышленных систем. В рамках проекта идёт создание на базе решения PCVue для АСУ ТП (разработки ARC Informatique) и Kaspersky Secure Hypervisor продукта, позволяющего вывести кибербезопасность АСУ ТП на новый уровень для обеспечения надёжной, стабильной и безопасной работы промышленных систем.

KasperskyOS®

Подробнее на os.kaspersky.ru

www.kaspersky.ru