

PERIMETRIX SAFESPACE™

УПРАВЛЕНИЕ
КОНФИДЕНЦИАЛЬНОСТЬЮ
ЦИФРОВЫХ АКТИВОВ

PERIMETRIX SAFESPACE™

Perimetrix SafeSpace™ – комплексное программное решение управления электронными данными, позволяющее обеспечить конфиденциальность и целостность электронной информации ограниченного доступа при ее хранении, обработке и передаче.

В основе решения лежат **концепция управления жизненным циклом** информации ограниченного доступа и уникальная **технология контроля перемещений электронной информации**. Применяя механизм настраиваемых **разрешительных политик хранения, обработки и передачи классифицированных данных**, Perimetrix SafeSpace™ обеспечивает защищенное исполнение пользователем и приложениями легитимного

рабочего процесса, при этом ограничивая всю иную, не предусмотренную политиками активность пользователей и приложений. Применение политик происходит динамически, в момент доступа к классифицированным электронным данным.

Программный комплекс сертифицирован **ФСТЭК России** (Сертификат № 3658 от 15.11.2016 г. действителен до 15.11.2019 г. соответствие РД, ТУ и НДВ4). Внедрение **Perimetrix SafeSpace™** позволяет выполнять требования Федерального закона «Об информации, информационных технологиях и защите информации» от 27.07.2006 г. № 149ФЗ и Федерального закона «О коммерческой тайне» от 29.07.2004 г. № 98ФЗ.

На всех стадиях жизненного цикла электронной конфиденциальной информации Perimetrix обеспечивает тот уровень ее безопасности, что и в бумажном режимном делопроизводстве, сохраняя в то же время гибкость, скорость и удобство электронной среды.

Многомерная модель классификации
Может применяться многомерная модель классификации информации, учитывающая не только степень конфиденциальности данных, но и другие признаки.

Разрешительный принцип полномочий
Полномочия пользователей и приложений формулируются в виде явных прямых разрешений, а все остальные действия по умолчанию считаются запрещенными.

Универсальная модель принятия решений
Любое действие с защищаемой информацией представляется как перемещение из контейнера-источника в контейнер-получатель. Система сравнивает полномочия с меткой и решает – разрешить или заблокировать операцию.

Неотделимые классификационные метки
Классификационная метка наносится на файл на глубоком уровне хранения компьютерных данных и не может быть самостоятельно удалена пользователем.

Механизм наследования меток
При копировании защищаемой информации из документа в документ или сохранении в виде новой копии классификационная метка будет унаследована.

Криптографическая защита данных
Для передачи ценных файлов может применяться шифрование путем помещения в криптоконтейнер, открыть который для извлечения из него данных можно лишь на контролируемом системной рабочей месте.

Преимущества:

- Единые политики режима классифицированной информации для всей организации
- Проактивный подход к предотвращению инцидентов безопасности
- Структуризация конфиденциальных корпоративных данных
- Интеграция в корпоративную информационную систему
- Сквозной аудит всех изменений в настройках системы
- Широкая масштабируемость и отказоустойчивость
- Низкая нагрузка на вычислительные ресурсы



Основные эффекты от внедрения

Для компании в целом:

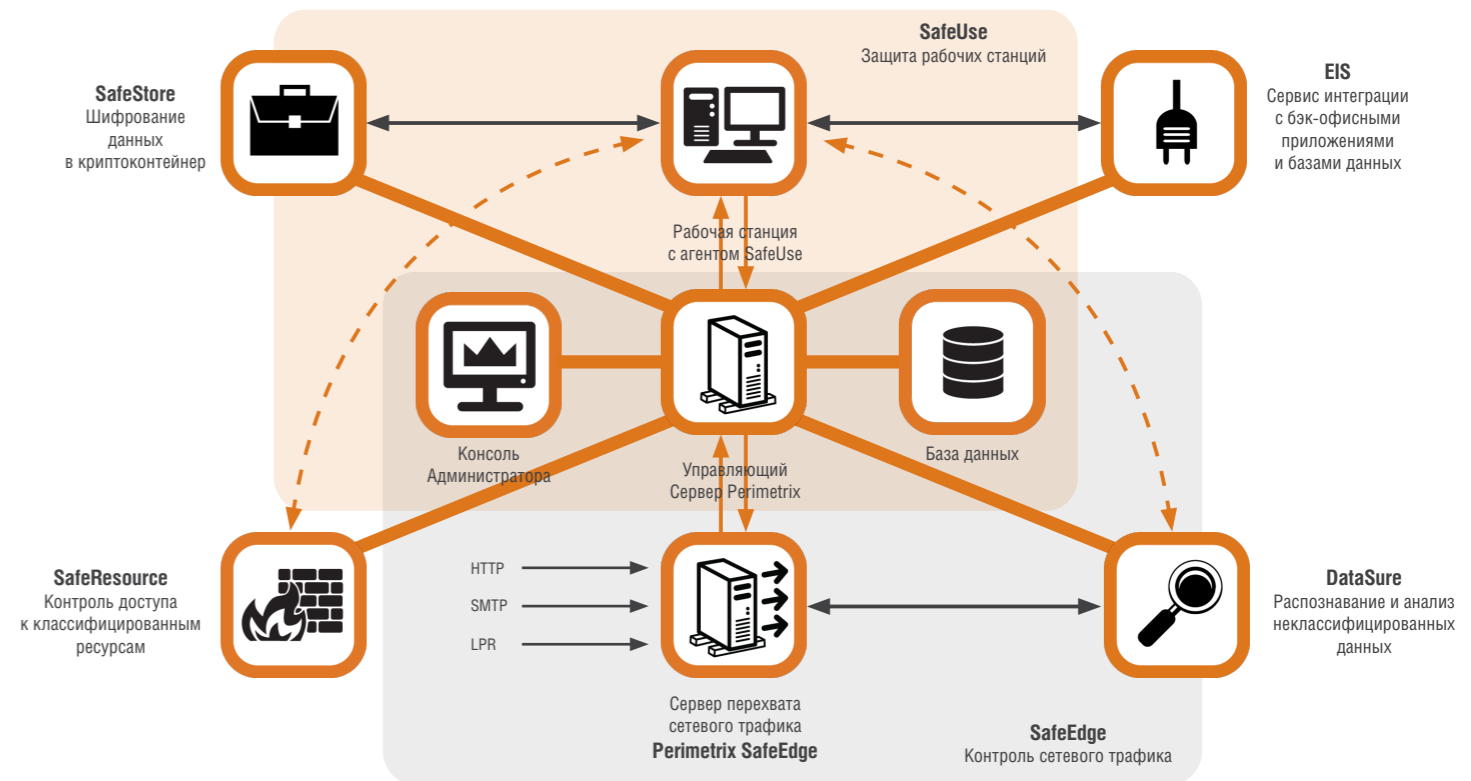
- Повышение качественных характеристик активов как драйвер повышения стоимости компании
- Создание рабочих процессов, способствующих соблюдению режима коммерческой тайны (КТ)
- Обеспечение работоспособности режима КТ при взаимодействии в группе компаний, с контрагентами
- Минимизация негативного влияния режима КТ на основную производственную деятельность

Для владельцев данных:

- Участие в принятии решений о ценности и конфиденциальности информации, ее категоризации
- Возможность самостоятельно назначать особый режим работы с данными, требующими защиты

Для службы безопасности/ИБ:

- Формализация понятия КТ, стандартизация содержащих ее документов и по возможности упрощение связанных с ней бизнес-процессов
- Четкие критерии для определения конфиденциальной информации, сокращение перечня информации, относящейся к КТ
- Снижение общего числа инцидентов и ресурсов, отвлекаемых на расследования, сокращение контрольных функций
- KPI специалистов блока безопасности основан не на фиксировании и расследовании утечек, а на предотвращении действий с КТ, не предусмотренных режимом



PERIMETRIX – российский разработчик систем управления классифицированными электронными данными, накопивший значительный опыт в обеспечении управления и защиты электронных данных, относящихся к коммерческой тайне, а в частности, к электронной конструкторской, дизайнерской и проектной документации на предприятиях машиностроения.

Компания основана в 2007 году командой профессионалов, стоявших у истоков создания современных систем защиты информации от внутренних угроз. Ее решения используются ведущими российскими и зарубежными компаниями и организациями в различных отраслях бизнеса.





Штаб-квартира Perimetrix
Россия, 119607, Москва,
Мичуринский проспект, д. 45
Телефон: +7 495 011 00 39
info@perimetrix.com
www.perimetrix.ru

Региональный центр
компетенций Perimetrix
Россия, 620142,
Екатеринбург,
улица Щорса, д. 7
Телефон: +7 343 287 11 76