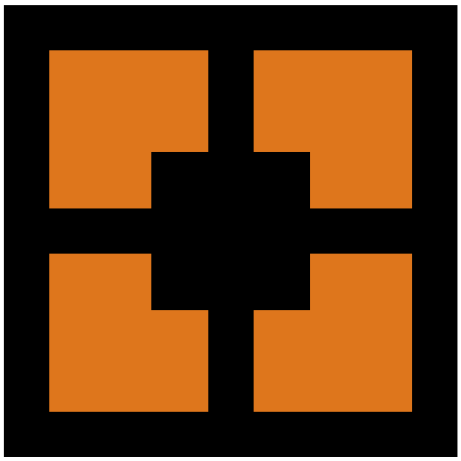
ОБЗОР ПРОГРАММНОГО
КОМПЛЕКСА



PERIMETRIX SAFESPACE™

КОМПЛЕКСНАЯ ЗАЩИТА
КОНФИДЕНЦИАЛЬНОСТИ
И ЦЕЛОСТНОСТИ ДАННЫХ

PERIMETRIX SAFESPACE™

Определение

Комплексное программное решение, обеспечивающее классификацию электронных данных и последующий контроль их целостности и конфиденциальности

Назначение

Управление и защита электронной информации при ее создании, хранении, использовании и передаче. Контроль соблюдения бизнес-сценариев, нуждающихся в обеспечении безопасности. Реализация режима коммерческой тайны при работе с конфиденциальными данными в электронной форме.

Функциональные возможности

- Многомерная классификация электронных данных
- Ограничение политиками разрешенных мест хранения и съемных носителей
- Блокирование несанкционированных действий с защищаемыми данными со стороны пользователей и программ
- Кодирование/шифрование защищаемых данных
- Автоматическая классификация производных данных
- Контроль печати документов ограниченного доступа
- Создание защищенных сетевых хранилищ данных ограниченного доступа
- Автоматическая классификация входящих данных
- Поиск и идентификация данных, нуждающихся в защите
- Надежное удаление данных без возможности восстановления
- Учет работы с данными ограниченного доступа

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.

Основные принципы

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

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

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

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

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 блокировать операцию.

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 системой рабочем месте.

PERIMETRIX SAFESPACE™

Решаемые задачи

1. Обеспечение сохранности информационных активов (интеллектуальной собственности, коммерческой тайны, банковской тайны, персональных данных и других видов конфиденциальной информации)
2. Защита информации от утечки и несанкционированного доступа со стороны легальных пользователей
3. Контроль над возможными каналами утечки: сеть, принтеры, сменные носители, порты рабочих станций
4. Гранулярное распределение полномочий по работе с информацией ограниченного доступа, в зависимости от назначенной категории и полномочий пользователя в информационной системе
5. Обеспечение непрерывности защиты путем автоматической классификации производных документов (появляющихся в результате обработки) и применения к ним соответствующих политик безопасности
6. Шифрование ценной информации, выходящей за пределы защищаемого периметра
7. Защита рабочих процессов от случайных отклонений или злоупотреблений со стороны пользователей

Область применения[1]

Целевыми потребителями **Perimertix SafeSpace™** являются предприятия и организации, использующие в своей деятельности данные ограниченного доступа, имеющие высокую внутреннюю ценность:

- Проектно-конструкторские организации и подразделения промышленных предприятий, разрабатывающие собственные решения и продукты,
- Коммерческие предприятия, действующие в жестком конкурентном окружении,
- Государственные и частные учреждения, имеющие дело с информацией, требующей защиты от несанкционированного распространения в соответствии с требованиями регуляторов:
  - персональные данные,
  - банковские данные,
  - медицинские данные и др.
- Любые другие организации, в деятельности которых необходимо обеспечение защиты от неправомерного использования или утечки таких видов данных как:
  - экономические, планово-статистические,
  - финансовые, юридические, судебные,
  - экологические, биологические, географические, геологические,
  - государственные, военные,
  - иные ценные данные ограниченного доступа.

[1] Описание решений на основе **Perimetrix SafeSpace™**, имеющих отраслевую специфику, и более полный список обслуживаемых SSBS (бизнес-сценариев, нуждающихся в обеспечении безопасности), см. на http://perimetrix.ru/

Сертификат ФСТЭК

В 2016 году Perimetrix SafeSpace™ 2.6 получил сертификат ФСТЭК № 3658, подтверждающий соответствие требованиям РД по НСД по 4 уровню контроля отсутствия НДВ и ТУ 5015 001 83140492 2016.

Российский разработчик

Perimetrix SafeSpace™ включен в Единый реестр российских программ за №4120 и отнесен к ПО «Системы мониторинга и управления», «Средства обеспечения информационной безопасности», «Информационные системы для решения специфических отраслевых задач».

Основные преимущества

Решение Perimetrix SafeSpace™ позволяет обойти ограничения стандартных технологий защиты от утечек в том виде, в котором они существовали до сегодняшнего дня. При помощи Perimetrix SafeSpace™ организация любого масштаба сможет построить простую, надежную и удобную систему защиты от внутренних нарушителей, поставить точку в решении проблемы защиты конфиденциальности и целостности данных.

- **Единые политики режима классифицированной информации для всей организации**
  Решения Perimetrix обеспечивают защиту классифицированной информации с помощью механизмов ее непрерывного контроля и мониторинга на протяжении жизненного цикла. Инструменты Perimetrix позволяют обрабатывать классифицированные данные в строгом соответствии с требованиями корпоративного режима безопасности, автоматически блокируя несоответствующие политикам действия.

- **Проактивный подход к предотвращению инцидентов безопасности**
  В отличие от получивших широкое распространение решений по мониторингу действий пользователей, применяемых как средство борьбы с утечками данных, Perimetrix не пытается реагировать на запрещенные действия, выполненные пользователями, а заранее блокирует возможность их совершения.

- **Структуризация корпоративного контента**
  Perimetrix позволяет привести в порядок корпоративный контент, классифицировать данные и выявить наиболее ценные объекты защиты. Сегментированный подход к защите информации различных классов снижает стоимость используемых средств, сосредотачивая главные усилия на защите наиболее важных ресурсов.

ОБЗОР ПРОГРАММНОГО КОМПЛЕКСА

PERIMETRIX SAFESPACE™

- **Интеграция в корпоративную информационную систему**
  Информация наиболее уязвима при переходе из структурированных и защищенных хранилищ (системы ЭДО, базы данных, ERP-системы и др.) в плохо структурированные формы (текстовые файлы, таблицы и т.д.). Perimetrix тесно интегрируется с гетерогенными корпоративными средами хранения и обработки данных (ERP, ЭДО, RDBMS, CRM, HRMS и проч.) и продолжает защищать данные, которые мигрируют в пользовательские приложения.

- **Сквозной аудит всех изменений в настройках системы**
  Все изменения в настройках, политиках и справочниках программного комплекса сохраняются в виде последовательных конфигурационных копий. Это дает возможность защититься от сговора администратора со злоумышленником и отследить историю внесенных изменений.

- **Широкая масштабируемость и отказоустойчивость**
  Серверная часть решения Perimetrix разворачивается на узлах кластера. При росте нагрузке достаточно добавить в кластер еще один сервер. Благодаря применению кластерной архитектуры достигается и высокая отказоустойчивость всей системы. Если какие-либо узлы выходят из строя, нагрузка перераспределяется между оставшимися машинами.

- **Низкая нагрузка на вычислительные ресурсы**
  Проверка легитимности перемещений информации, состоящая лишь в сравнении допустимых и актуальных уровней полномочий элементов универсальной модели принятия решений, не требует сколь-либо значительных вычислительных ресурсов компьютера пользователя, в отличие от кропотливой рутины вероятностных методов классификации контента, практикуемых стандартными средствами предотвращения утечек.

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

Примеры внедрения

Защита проектно-конструкторской и иной документации
Завод несет потери из-за контрафакта, теряет клиентов из-за того, что создаваемые ноу-хау используются небольшими фирмами, получающими доступ к разработкам без оплаты роялти владельцу интеллектуальной собственности. Руководство требует надежно защитить новую техническую документацию и работу высокооплачиваемых специалистов.

При помощи Perimetrix чертежи и рабочие документы, создаваемые на рабочих местах конструкторов, проектировщиков и дизайнеров, ограничены в распространении рамками предприятия.

Защита информации, создаваемой топ-руководителями
Руководители организации на своих рабочих местах постоянно создают, редактируют и обмениваются информацией, содержащей элементы, части, прообразы коммерческой тайны. Однако только конечные документы получают статус подлежащих защите.

При помощи Perimetrix руководители получат возможность защищать ценные для них рабочие данные с момента их создания. При этом система поможет определить наличие копий и схожих документов случайных местах хранения и также защитить их.

Конкурентная тендерная заявка
Начинает готовиться широким кругом лиц из несекретных данных. Но на заключительном этапе приобретает конфиденциальный характер и может формироваться лишь несколькими доверенными лицами.

При помощи Perimetrix можно временно ограничить круг лиц, имеющих доступ к тендерной документации, на то время, пока эти данные чувствительны к утечке.

Несанкционированная деятельность сотрудника
Пользуясь рабочим местом, дорогостоящим программным обеспечением и тратя оплаченное рабочее время, сотрудник выполняет личные заказы.

При помощи Perimetrix все создаваемые информационные объекты маркируются как собственность организации и запрещены к самовольному выносу за пределы компании.

Наши клиенты

МОСИНЖПРОЕКТ
ЗиК
РусГидро
СФ Совет Федерации Федерального Собрания Российской Федерации
Пермский завод МАШИНОСТРОИТЕЛЬ
financial intelligence centre REPUBLIC OF SOUTH AFRICA
АВТОВАЗ
ИНТЕГРАЛ INTEGRAL
ГМОЗК
LIGHTSTONE

PERIMETRIX SAFESPACE™

Дополнительные сценарии применения

1. Выполнение политики хранения определенных данных только в назначенном месте
2. Защита данных третьих лиц, автоматическая криптозащита на входе, регламентированное снятие защиты при передаче третьим лицам, контроль точки перехода
3. Инвентаризация информационных активов, составление карты классифицированной информации
4. Контроль защищаемых файлов, выбор разрешенных принтеров в зависимости от классификационного уровня документа
5. Защита данных, поступающих из бэк-офисных систем (ERP, CRM), защита выгрузок из БД, данных внутренних портальных систем

Порядок внедрения

Типовое внедрение Perimetrix SafeSpace™ на предприятии предполагает выполнение следующих этапов:

1 этап. Организация проекта и создание демо-стенда

- Создание совместной рабочей группы со специалистами заказчика
- Разработка и подписание Устава проекта
- Установка системы Perimetrix SafeSpace™ на демо-стенде
- Обучение специалистов заказчика, включенных в рабочую группу

Итоги 1 этапа:

- ✓ Определен состав рабочей группы
- ✓ Создан демо-стенд с системой Perimetrix SafeSpace™ на инфраструктуре заказчика
- ✓ Собственные специалисты заказчика способны транслировать политики безопасности предприятия во внутренние настройки системы

2 этап. Разработка модели защиты коммерческой тайны

- Сбор данных о рабочих процессах в аспекте движения данных, представляющих ценность, в том числе:
  - о характере ценных данных бизнес-процессах, в которых они используются
  - о перечне и полномочиях пользователей, работающих с такими данными
  - о программных средствах, используемых для их создания и обработки
  - о топологии компьютерной сети, местах хранения и каналах передачи ценных данных
  - о возможных сценариях утечки
- Разработка Модели защиты и ее документирование, включающее:
  - определение объектов защиты и составление классификатора данных
  - определение пользователей и групп и их полномочий при работе с КД
  - описание политик и процедур в части обработки, хранения и передачи КД, определяющее допустимые места хранения, форматы, приложения для обработки, каналы передачи КД
  - моделирование новых и скорректированных бизнес-процессов и процедур в части работы с КД

Итоги 2 этапа:

- ✓ Определена и построена модель защиты, включающая:
  - категории и правила классификации
  - политики обработки ценных данных
  - полномочия пользователей, приложений
  - бизнес-процессы и процедуры, выполняемые под контролем системы

3 этап. Настройка и проверка Модели защиты информации на тестовом стенде

- Создание тестового стенда, включающего типовое защищенное рабочее место сотрудника
- Программирование политик, предусмотренных Моделью защиты
- Проверка корректности и безопасности выполнения бизнес-процессов на тестовом стенде
- При необходимости внесение изменений в настройки политик и описание Модели защиты

Итоги 3 этапа:

- ✓ Создан тестовый стенд с типовым рабочим местом заказчика
- ✓ Выявлены и учтены замечания к настройкам Модели защиты
- ✓ Реализовано выполнение защищенных бизнес-процессов на тестовом стенде

4 этап. Разработка организационно-распорядительной документации

- Разработка регламента работы с электронными данными
- Разработка инструкции для пользователей
- Разработка инструкции для специалиста по безопасности

Итоги 4 этапа:

- ✓ Разработана организационно-распорядительная документация

5 этап. Опытная эксплуатация системы и сдача проекта

- Настройка системы на рабочем сервере и установка агентов на рабочие станции
- Первичная инвентаризация и классификация информационных ресурсов
- Обучение пользователей, опытная эксплуатация системы
- Корректировка настроек и процедур по результатам опытной эксплуатации
- Корректировка и утверждение организационно-распорядительной документации
- Введение периодических заданий в систему

Итоги 5 этапа:

- ✓ Утверждена организационно-распорядительная документация
- ✓ Пользователи предприятия обучены работе в защищенном режиме
- ✓ Выявлены и замечания и выполнены корректировки работы системы
- ✓ Система применена к рабочим ресурсам
- ✓ Специалисты заказчика самостоятельно выполняют обслуживающие процедуры и вносят необходимые изменения в систему

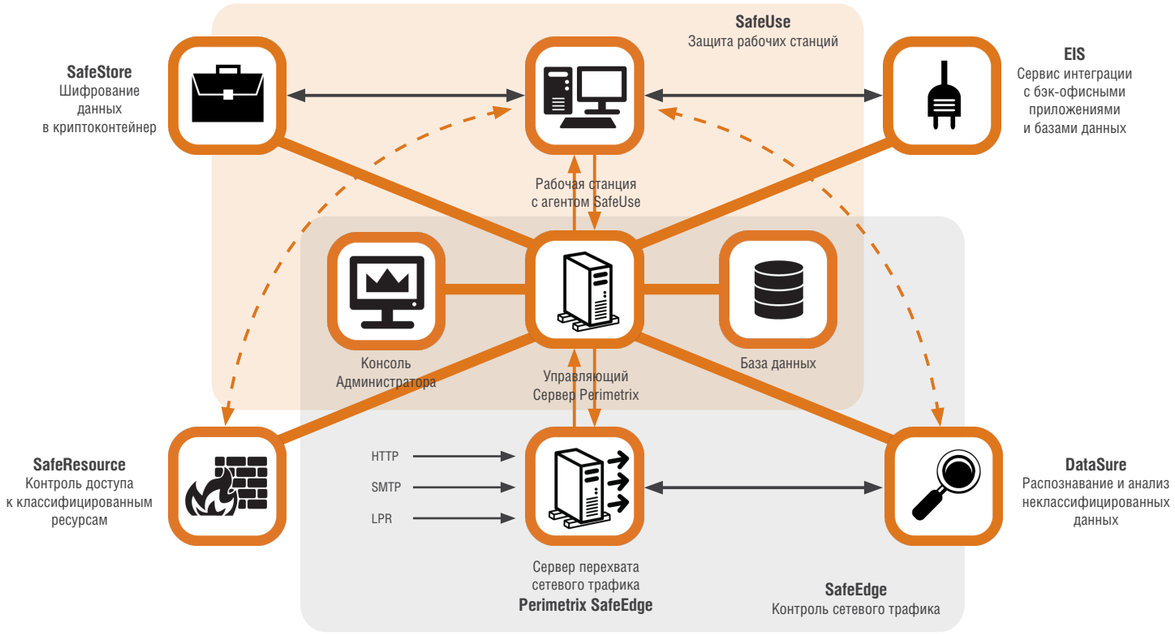
Возможности интеграции

Предусмотрена возможность интеграции с гетерогенными корпоративными средами хранения и обработки данных (ERP, ЭДО, RDBMS, CRM, HRMS и проч.).

ОБЗОР ПРОГРАММНОГО КОМПЛЕКСА

PERIMETRIX SAFESPACE™

Основные компоненты программного комплекса



1. SafeUse™
— защита классифицированных данных во время обработки на компьютерах пользователей

2. SafeEdge™
— контроль сетевого трафика (SMTP, HTTP, IM, сетевые принтеры) на наличие конфиденциальных данных

3. SafeStore™
— криптографическая защита данных в местах хранения (сертифицированные в РФ и Республике Беларусь криптобиблиотеки)

4. SafeResource
— защита серверов от доступа с «небезопасных» клиентов (станции без агента, мобильные устройства и т.п.)

5. Enterprise Integration Server
— интеграция и защита данных и приложений класса ERP, CRM

6. DataSure
— распознавание и анализ неклассифицированных данных для идентификации уровня конфиденциальности

Общие требования к программно-аппаратному обеспечению

Web-интерфейс консоли управления/Серверная часть
- Процессор 2XCore2Quad Xeon, 1,6GHz, 2GB RAM, 500 GB HDD, NIC Ethernet 1000
- Любая ОС, поддерживающая JAVA
- Java JRE 6.0 update 7 и выше
- Apache Tomcat 6.0.14 и выше

Сервер основных служб
- Процессор 2XCore2Quad Xeon, 2GHz, 4GB RAM, 500GB HDD, NIC Ethernet 1000
- Linux OS, Sun Java JRE 6u13

Клиентская часть
- Любая рабочая станция под управлением клиентских ОС Microsoft Windows XP, Vista, Win 7, 8, 10, а также серверных ОС Windows Server 2008, 2012 и 2016. Требования к аппаратной части определяются операционной системой

Сервер СУБД
- Процессор 2xCore2Quad XEON 2 GHz, 4 Gb RAM, 2 Tb HDD, NIC Ethernet 1000
- Любая СУБД с поддержкой Hibernate (Oracle, DB2, Sybase, MS SQL Server, PostgreSQL, MySQL и т.д.)

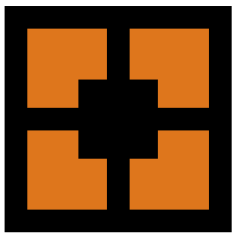
Сервер перехвата сетевого трафика
- Процессор 2XCore2Quad Xeon, 2GHz, 4GB RAM, 500GB HDD, NIC Ethernet 1000
- Linux OS, Sun Java JRE 6u13
- NetFilter libraries libnet, libnfnetlink, libnetfilter_conntrack

Различные сервисы могут быть развернуты как на одном физическом сервере, так и на нескольких. Выбор аппаратной части серверов и установка СУБД должны производиться по рекомендациям фирмы-разработчика СУБД.

Дополнительно при использовании модуля **SafeStore™:**

Серверная часть
- Криптопровайдер с поддержкой Java Cryptography Architecture (JCA). Доступны КриптоПро JCP 1.0, Avest 1.01.RC3, Bouncy Castle (открытый код), и встроенные в JRE криптопровайдеры Sun.

Клиентская часть
- Криптопровайдер с поддержкой Microsoft CryptoAPI. Доступны библиотеки КриптоПро CSP 3.0 (отвечает требованиям законодательства РФ и сертифицирована ФСБ и ФСТЭК) и Microsoft Enhanced Cryptographic Provider (входит в комплект поставки Windows)



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