ACCESSDATA

ACCESSDATA

Решения для расследования инцидентов и сбора доказательств

AD Enterprise

Forensic Toolkit (FTK)

AD eDiscovery

AD Lab

Cross Technologies

AD ENTERPRISE

Появление больших объемов данных стало причиной различных трудностей, возникающих при проведении внутренних расследований с использованием цифровых данных.

В мире, переполненном информацией, специалисты в области цифровой криминалистики столкнулись с самыми разными проблемами. Филиалы, огромные штаты компаний и сотрудники, работающие удаленно, — все это серьезно усложняет сбор и анализ данных. Внутренние расследования, проверки или судебные разбирательства имеют жесткие временные рамки, которые сложно соблюдать с использованием устаревших решений для компьютерно-технической экспертизы, и зачастую требуют совместной работы. Когда вам необходимо рассмотреть проблему, связанную с персоналом, проверить достоверность предоставленных заявлений, изучить запросы государственных органов или решить вопросы, связанные с соблюдением норм, вам понадобится решение, которое способно быстро находить данные, оперативно передавать их соответствующим сотрудникам для анализа и гарантировать целостность этих данных.

ЧТО ТАКОЕ AD ENTERPRISE?

AD Enterprise, в основе которого лежит технология FTK, используется компаниями из списка Fortune 1000 и различными государственными органами для проведения внутренних расследований, целью которых является идентификация, сбор, анализ и целевое восстановление цифровых данных. Поскольку это решение способно получать доступ к компьютерам во всей вашей компании, ИТспециалисты и цифровые криминалисты могут удаленно просматривать и получать данные с рабочих станций, независимо от их местоположения. Обеспечение защиты интеллектуальной собственности, сокращение расходов и совместная работа всех отделов над происшествиями еще никогда не была такой простой!

БОЛЬШЕ, ЧЕМ ПРОСТО РЕШЕНИЕ ДЛЯ ВНУТРЕННИХ РАССЛЕДОВАНИЙ

Помимо того, что AD Enterprise является решением для расследования внутренних происшествий, таких как правонарушения сотрудников и несоблюдение установленных норм, оно также способствует сотрудничеству всех отделов и может отслеживать угрозы и исправлять недостатки систем безопасности.

Защита вашего предприятия

Решение AD Enterprise создано для устранения угроз, независимо от их источника, и исправления недостатков систем безопасности, причем все эти операции могут быть выполнены централизованно из одного места, одного централизованного офиса.

Внешние угрозы

- **Хакерские атаки.** Сканирование нескольких машин одновременно для определения количества нарушений и анализа их первопричин.
- **Вредоносные программы.** Сканирование всей сети для поиска известных и неизвестных вредоносных процессов и файлов DLL.
- **Поврежденные данные.** Создание профиля угрозы и выполнение проверки для выявления всех зараженных компьютеров.
- **Предупреждения при обнаружении вторжений.** Отображение предупреждений сети или системы при обнаружении подозрительных входящих и исходящих сетевых процессов.

Внутренние угрозы

- **Мониторинг данных.** Корреляция пользовательской активности с помощью предупреждений об используемых данных и компьютерно-технический анализ для сохранения соответствующей информации.
- **Нарушения использования компьютеров.** Сканирование сети для поиска неодобренных процессов и просмотр подключенных хранилищ для выявления нарушений при использовании компьютеров.

- **Интеллектуальное воровство.** Быстрые и тщательные проверки нескольких пользователей с основным вниманием к их файлам и электронной почте.
- **Правонарушения сотрудников.** Масштабные скрытые экспертно-криминалистические расследования для выявления правонарушений.

Совместная работа и сокращение задействованных ресурсов

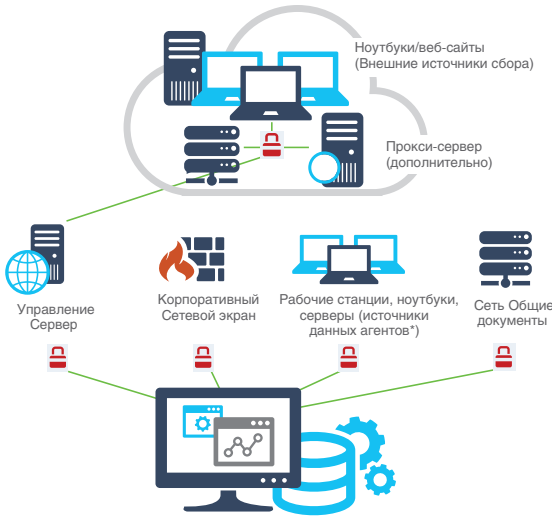
ИТ-специалисты, юристы, сотрудники отдела регулирования, отдела кадров и службы безопасности обладают подробной информацией о рассматриваемом деле и даже более тесно взаимодействуют с защищенной серверной базой данных. Только AccessData предлагает общую информационную базу данных в течение всего судебного разбирательства.

ОБЛАСТЬ ОХВАТА

Решения AccessData обеспечивают область охвата всей сети при расследованиях, поддерживая возможность проведения судебной экспертизы в следующих операционных системах:

- Windows
- Linux
- Mac
- UNIX
- Android
- iOS
- BlackBerry

Многие компании используют сложные структуры для доступа к данным и их хранения. Решения AccessData способны предварительно отображать и получать данные из удаленных точек, которые хранятся как на компьютерах, установленных в разных офисах, так и в облачных средах. Решения AccessData устраняют необходимость покидать пределы компании при проведении компьютерно- технической экспертизы.



AD Enterprise позволяет проводить расследования за пределами сетевого экрана. Удаленный доступ, дистанционная передача данных или работа сотрудников на дому более не будут препятствиями для проведения всесторонних расследований.

БЕЗОПАСНОСТЬ

Решения AccessData позволяют проводить расследования за пределами вашего сетевого экрана. Вся информация, используемая для расследования, надежно защищена от постороннего доступа при хранении для судебного разбирательства. Обеспечивается соответствие требованиям Sarbanes-Oxley, PCI, HIPPA, FISMA и любым другим внутренним нормам безопасности, которые обязательны в вашей компании.

FORENSIC TOOLKIT (FTK)

Быстрый и тщательный сбор доказательств: программное средство компьютерно-технической экспертизы, ставшее стандартом на мировом уровне

С ростом объема данных, поступающих из разнообразных устройств и систем, становится все сложнее оперативно и эффективно искать и собирать цифровые доказательства. Правоохранительным органам и коммерческим компаниям приходится обрабатывать огромное количество устройств и источников, чтобы найти нужную информацию в море данных, — а это непростая задача. Интегрированное решение для компьютерно-технической экспертизы FTK позволяет сократить время и ресурсы, необходимые для расследования. Ведущие цифровые криминалисты используют именно это решение.

ЧТО ТАКОЕ FTK?

FTK — признанное судебной системой и отмеченное наградами решение для проведения расследований в цифровой среде. Это решение отличается скоростью, стабильностью и простотой использования. Всего одно приложение позволяет быстро выявлять, собирать и анализировать цифровые доказательства в разных системах и на разных устройствах, способных создавать наборы данных, передавать или сохранять данные. Решение FTK имеет интуитивно понятный интерфейс, позволяет анализировать электронную почту, настраивать отображение данных, быстро обрабатывает данные и работает стабильно. При этом FTK закладывает структуру, на основе которой система сбора доказательств может совершенствоваться и расти вместе с вашей организацией или учреждением.

ОТЛИЧИЯ FTK ОТ ДРУГИХ ПРОДУКТОВ НА РЫНКЕ

Работа на основе базы данных: единая база для расследования

Все цифровые доказательства сохраняются в единой базе данных, к которой могут обращаться различные группы специалистов, чтобы получать самые актуальные сведения. За счет отказа от создания нескольких наборов данных можно сократить расходы и время на расследование, а также упростить работу. Расследованию не будут мешать неполадки, типичные для других доступных на рынке инструментов, обращающихся к памяти, — например, обработчики данных могут не прерывать своей деятельности даже в случае сбоя графического интерфейса. И самое главное: решение позволяет всем участникам расследования активно взаимодействовать благодаря постоянному обмену информацией между решениями AccessData для проведения экспертизы и электронного обнаружения данных.

Высокая скорость обработки и надежная среда

Цифровые доказательства обрабатываются сразу, поэтому на этапе анализа не приходится ждать, пока будет завершен поиск. Решение FTK обеспечивает самую быструю, точную и последовательную обработку данных за счет распределения этого процесса и полной поддержки многопоточности и многоядерности.

Зачем нужна поддержка многопоточности и многоядерности? Решение FTK полностью задействует аппаратные ресурсы, что повышает его надежность в случае программных или аппаратных неполадок, а также увеличивает скорость обработки данных.

Ускоренный поиск нужной информации

Индексирование выполняется заранее, поэтому фильтрация и поиск проходят быстрее, чем при использовании любого другого решения. А в новой версии FTK 6.0 создается единый индексный файл для всех этапов, будь то расследование или проверка документов, — это значит, что индексный файл не нужно дублировать или создавать заново. Важнее всего то, что пользователи получают единообразные результаты поиска как в FTK, так и в Summation.

ДРУГИЕ ВАЖНЫЕ ОСОБЕННОСТИ

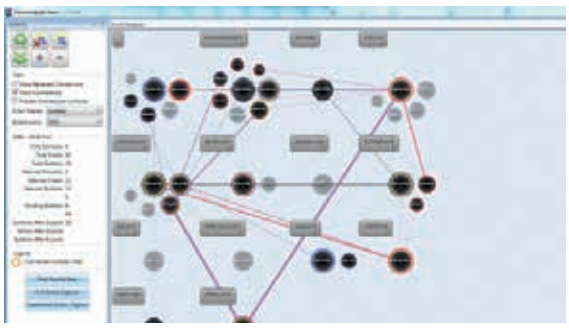
FTK позволяет создавать образы и обрабатывать данные самых разных типов: от криминалистических образов до архивов электронной почты и информации с мобильных устройств, — а также анализировать реестр, раскрывать пароли и создавать отчеты. И все это при помощи единого решения.

Анализ данных на удаленных машинах

При использовании корпоративной версии решения пользователи могут предварительно просматривать, получать и анализировать доказательства с удаленных компьютеров в вашей сети.

Визуализация

Решение позволяет автоматически выстраивать временные шкалы и графически иллюстрировать взаимоотношения между заинтересованными сторонами. Визуализация данных электронной почты, социальных связей и файлов позволяет отображать информацию в различных форматах, включая временные шкалы, кластерные и круговые диаграммы, геолокационные карты и тому подобное, чтобы выявить взаимосвязи и найти ключевую информацию. Результаты можно отобразить в отчетах, удобных для юристов, ИТ-директоров и других участников расследования.



Анализатор социальных связей позволяет просматривать коммуникации по электронной почте на уровне домена, а также переходить на уровень отдельных владельцев данных и просматривать коммуникации между конкретными лицами.

Доказательства из браузеров и электронной почты на базе веб-интерфейса

Почти каждое расследование включает анализ веб-артефактов. В кэш браузеров записываются адреса сайтов, на которые заходил подозреваемый, электронная почта на базе веб-интерфейса может помочь доказать умысел или установить связь с другими событиями, разговоры в средствах мгновенного обмена сообщениями и социальных сетях также могут содержать важные доказательства. Обработка доказательств позволяет разделить по категориям и организовать файлы, чтобы их было легко просматривать.

Раскрытие и восстановление паролей

Передовое решение позволяет просматривать файлы, защищенные паролями, при помощи технологии раскрытия и восстановления.

Обнаружение непристойных изображений

Технология распознавания изображений различает телесные тона и автоматически выявляет изображения с возможным порнографическим содержанием.

Фильтрация и анализ вредоносных файлов

В виде интегрируемого дополнения к FTK доступна платформа Cerberus для автоматической фильтрации вредоносных файлов. Cerberus представляет собой первый уровень защиты при сохранении образов неизвестных устройств. Решение позволяет выявлять опасные файлы после обработки данных в FTK. Пользователь видит, какие файлы потенциально инфицированы, и может отказаться от их экспорта. Cerberus — одно из средств защиты от потенциально вредоносных файлов. Оно позволяет специалистам:

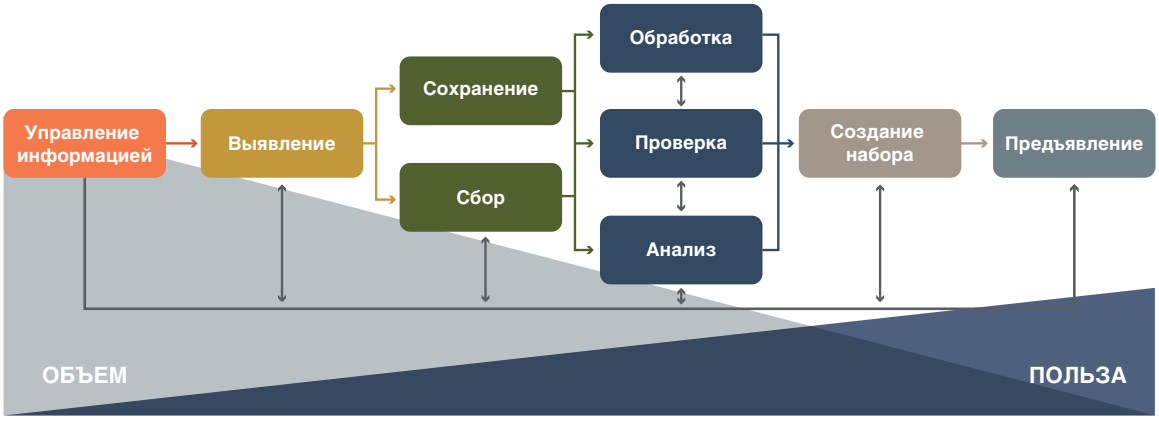
- при помощи комплексного анализа заранее выявлять факторы, ведущие к нарушению безопасности, — до полномасштабной вирусной атаки;
- укреплять защиту от угроз и предотвращать запуск вредоносных программ — при помощи передовой технологии белых списков;
- предпринимать действия прежде, чем возникнет нарушение безопасности, — в отличие от продуктов конкурентов, Cerberus не использует «песочницу» и сигнатурные методы.

AD EDISCOVERY

Простой и эффективный поиск в масштабах компании, целевой сбор достоверных данных для компьютерно-технической экспертизы, систематизация, хранение для судебного разбирательства, обработка, оценка данных и полная юридическая проверка — при разумных расходах и с меньшим риском.

Общепринятый порядок обнаружения электронных данных определяется эталонной моделью EDRM и не зависит от того, какие инструменты использует организация. В рамках EDRM данные требуется как минимум выявить, затем собрать, обработать для анализа, проверить внутри организации и отобрать нужные. Этот подготовленный набор данных необходимо импортировать в средство юридической проверки, используемое внешним юрисконсультом.

Решение AD eDiscovery и модель EDRM



ЧТО ДАЕТ ВАШЕЙ ОРГАНИЗАЦИИ РЕАЛИЗАЦИЯ ВСЕХ ЭТАПОВ ОБНАРУЖЕНИЯ ЭЛЕКТРОННЫХ ДАННЫХ НА ЕДИНОЙ ПЛАТФОРМЕ?

- **Снижение риска для компании.** Данные не передаются между технологиями и решениями разных поставщиков благодаря единому, безопасному, комплексному решению. Решение также защищает данные от порчи, потери и кражи.
- **Обеспечение соответствия нормам.** Достижение систематичности и юридической обоснованности сохранения данных для судебных разбирательств согласно мировым требованиям, а также регулятивным правительственным нормам.
- **Повышение скорости реагирования.** Быстрое получение, сохранение и анализ данных из широкого ряда хранилищ и целевых систем с использованием испытанной и широко распространенной технологии компьютерно-технической экспертизы.
- **Снижение общей стоимости.** Обработка всей потенциально значимой информации: структурированной и неструктурированной, внутри и за пределами организации, — при помощи единого интегрированного решения.

AD eDiscovery находит и собирает нужные данные, обрабатывая широчайший ряд структурированных и неструктурированных источников на базе любой из платформ, доступных на рынке. С помощью простых в использовании шаблонов, учитывающих стандартные рабочие процессы, AD eDiscovery собирает данные без установки агентов в следующих средах:

- Box
- CloudMail (протоколы POP и IMAP)

- Сервисы CMIS
- Documentum
- DocuShare
- Domino (Notes)
- Druva (клиент AD)
- Enterprise Vault
- Веб-службы Exchange (2010 SP1, 2013, O365, SilverSky)
- Exchange MAPI (2007, 2010, 2013)
- Google Диск
- Gmail (Administrative)
- Microsoft Office 365 (Exchange [электронная почта и календарь], SharePoint и OneDrive)
- Система управления корпоративным контентом OpenText (LiveLink)
- SharePoint (2007, 2010, 2013, O365)
- WebCrawler (Web 1.0)

ПРЕИМУЩЕСТВА AD EDISCOVERY

AD eDiscovery — единая, полностью интегрированная платформа, позволяющая обнаруживать достоверные данные для компьютерно-технической экспертизы во всей организации: искать, собирать данные, сохранять их для судебного разбирательства, обрабатывать и оценивать, а также выполнять их полную юридическую проверку.

AccessData Group стоит у истоков технологий для судебных разбирательств и компьютерно-технической экспертизы и работает в этой области уже более 25 лет. За это время компания создала и отдельные продукты, и решения корпоративного класса, синергичное взаимодействие которых помогает в обнаружении электронных данных для расследования гражданских и уголовных правонарушений. Решения AccessData поддерживают все этапы EDRM: от выявления до финальной проверки и подготовки к предъявлению. Благодаря единой платформе для всех продуктов и общей серверной базы данных, в основе которых лежит созданная компанией технология компьютерно-технической экспертизы Forensic Toolkit (FTK), решения для обнаружения электронных данных помогают группам по судебным разбирательствам контролировать объем данных, снижать риск, связанный с их перемещением, и сокращать расходы на обнаружение. Программным решениям AccessData, а также высококлассным продуктам и услугам для компьютерно-технической экспертизы, созданным компанией, доверяют более 130 000 клиентов в разных странах мира: корпорации, юридические фирмы, правоохранительные и другие государственные органы.

НОВАЯ ВЕРСИЯ ПРОДУКТА: AD EDISCOVERY 6.1

Последняя версия AD eDiscovery позволяет быстрее выполнять сбор данных из более широкого спектра источников, в том числе из Office 365. Автоматизировано большее количество задач, благодаря чему уменьшилось количество требуемых действий и сократился временной промежуток между сбором данных и их анализом. Добавлены улучшения, призванные повысить защиту целостности данных.

Последние улучшения

- Поддержка Office 365 Exchange (электронной почты и календаря), SharePoint и OneDrive для бизнеса
- Более высокая скорость индексирования
- Повышенная прозрачность конфигурации серверов
- Возможность задавать график автоматического обновления собранных данных
- И многое другое!

Подробнее о решении AD eDiscovery см. на сайте accessdata.com/solutions/e-discovery/ADeDiscovery

AD LAB

Когда расследования выходят за рамки вашей компании или учреждения — разделяй и властвуй.

При проведении компьютерно-технической экспертизы занято большое количество специалистов, среди которых цифровые криминалисты, представители службы безопасности, ИТ-специалисты, сотрудники отдела кадров, юристы и эксперты. Обеспечение согласованности, комплексности и целостности данных является непростой задачей. Решение AD Lab компании AccessData упростит разделение рабочих обязанностей при проведении расследования любого масштаба. При разработке данного решения основное внимание уделялось совместной работе. Большое количество настроек пользовательских элементов управления, централизованная база данных, удобный доступ с помощью веб-интерфейса и управление несколькими делами отличительная особенность решения, которое поможет даже при самых сложных кейсах.

ЧТО ТАКОЕ AD LAB?

AD Lab, в основе которой лежит технология FTK, является платформой для проведения расследований, которая обеспечивает разделение рабочих обязанностей, централизованное управление делами и доступ с использованием веб-интерфейса. Вместо снижения темпов работы, связанного с ожиданием результатов, которые необходимы для расследования, вы можете управлять всеми процессами из единой базы данных, используя различные уровни контроля пользователей. При необходимости дополнительных ресурсов для обработки больших объемов данных, функция распределенной обработки информации, реализованная в AD Lab, задействует мультиаппаратные средства, что обеспечит требуемую мощность и позволит сократить время рассмотрения дела.

СОВМЕСТНАЯ РАБОТА В AD LAB

Компьютерно-техническая экспертиза требует привлечения большого количества специалистов. Принцип «разделяй и властвуй» позволяет обеспечить доступ всех сотрудников к общей информационной базе данных с помощью веб-интерфейса AD Lab.

- **Назначение ролей.** Возможность предоставления каждому пользователю доступа только к тем данным, которые относятся к его области расследования. Эта эффективная фрагментированная система распределения ролей обеспечивает недоступность всей базы данных электронных доказательств для всех пользователей. Разделение доказательств создает более эффективный и безопасный рабочий процесс, тем самым позволяя привлекать к работе пользователей нетехнических специальностей без какой-либо угрозы для данных.
- **Совместная работа.** Централизованная архитектура и единая база данных обеспечивают согласованность информации для всех занятых сторон и позволяет максимально быстро обрабатывать дела. Благодаря системе анализа на основе веб-интерфейса пользователи нетехнических специальностей, например юристы, сотрудники отдела кадров и юридические консультанты, могут участвовать в процессе без каких-либо задержек, независимо от своего места расположения.
- **Простота использования.** Удобное решение, разработанное для доступа пользователей, не обладающих специальными знаниями.
- **Оптимизированная скорость анализа данных.** При расследовании некоторых дел необходимо обрабатывать огромные объемы данных, которые могут оказаться слишком велики для существующей рабочей среды. Платформа AD Lab предназначена для совместной работы и поддерживает распределение нагрузки среди всей группы серверов, а не используя только один из них. Помимо увеличения скорости анализа данных, вы также можете повысить надежность, используя систему с резервными обрабатывающими ресурсами, которые

задействуются в случае сбоев или неполадок в работе аппаратного или программного обеспечения.

- **Раскрытие и восстановление паролей.** Передовое решение для раскрытия и восстановления паролей.
- **Использование мастеров.** Криминалистический анализ на нескольких компьютерах и обработка, фильтрация и создание отчетов данных с использованием мастеров.
- **Интегрированные и расширенные возможности совместной работы.** Полная интеграция решений FTK, AD Enterprise и AD eDiscovery. Вся информация хранится в одной базе, что позволяет сократить время, уменьшить расходы и устранить трудности, возникающие при работе с делами.

ПОДДЕРЖКА И ОБУЧЕНИЕ

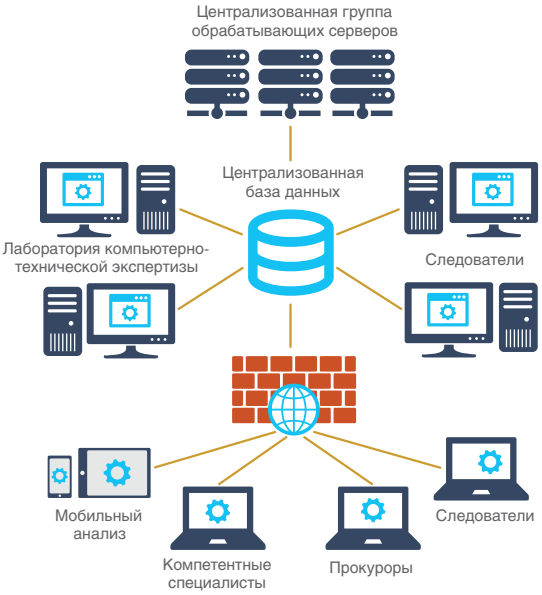
Мы стремимся предоставлять максимально эффективную техническую поддержку, а так же обучать основам работы с продуктами и совершенствовать их, чтобы затраты наших клиентов окупились как можно быстрее.

- Возможности поддержки представлены на веб-сайте http://marketing.accessdata.com/Support и включают в себя следующее:
- Техническая поддержка по телефону
- Портал базы данных, который содержит ответы на общие вопросы
- Форум, на котором пользователи могут оставлять вопросы и искать ответы
- Руководства пользователя, краткие справочные руководства руководства и многое другое!

Варианты для обучения доступны по адресу http://marketing.accessdata.com/ADTraining и сочетают уникальную методику обучения с самыми современными технологиями. Среди предлагаемых вариантов: личный учебный кабинет, обучение в режиме онлайн или с помощью нашей системы управления обучением (LMS). Для доступа к системе LMS перейдите по адресу http://marketing.accessdata.com/LMStraining

AD LAB | ПРИМЕР АРХИТЕКТУРЫ

Применяйте принцип «разделяй и властвуй», используя корпоративный подход к обработке больших объемов данных с помощью совместной работы и централизованного решения AD Lab.

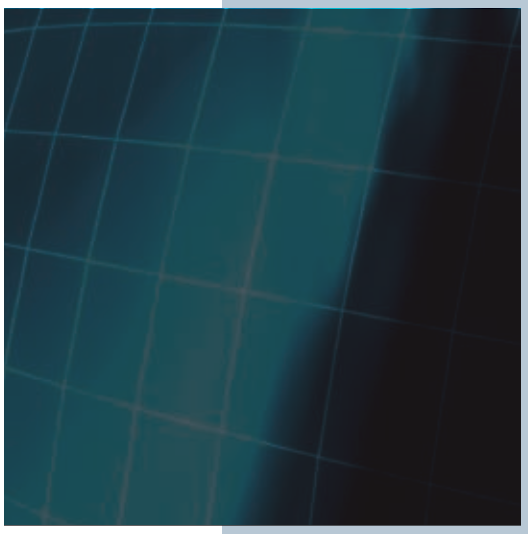


ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

Кросс технолоджис — эксклюзивный дистрибьютор решений компании AccessData.

Наличие необходимого пакета лицензий ФСТЭК России и ФСБ России позволяет **Кросс технолоджис** оказывать широкий спектр услуг по защите конфиденциальной информации — от разработки и сертификации средств защиты информации до их внедрения и последующего сопровождения.



Кросс технолоджис — это команда компетентных специалистов, решающих поставленные задачи на всех этапах сотрудничества.

Адрес: 115280, г. Москва,
ул. Ленинская слобода, д. 26,
БЦ «Омега-2», корпус С
Телефон: +7 (495) 741-88-64
E-mail: info@crosstech.su
www.crosstech.su