



**ФОРМУЛА ЭФФЕКТИВНОГО УПРАВЛЕНИЯ ДОСТУПОМ
IDM+PKI+SSO**

2013 г.

СИСТЕМА УПРАВЛЕНИЯ ДОСТУПОМ КАК ФУНДАМЕНТ ДЛЯ ВСЕЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Деятельность практически любого современного предприятия самым существенным образом зависит от его информационной системы (ИС). Бурное развитие ИС в последние десятилетия привело к сверхконцентрации в них всевозможных конфиденциальных данных. И сегодня необходимость защиты ИТ-инфраструктуры и прикладного ПО ни у кого не вызывает сомнений.

Неудивительно, что российские предприятия тратят огромные средства на внедрение различных организационно-технических средств защиты конфиденциальных данных, что позволяет отечественному рынку ИБ устойчиво расти более чем на 30% ежегодно. Такая динамика создает ощущение благополучия, однако практика показывает, что все эти дорогостоящие системы почему-то не могут сбить волну компьютерных преступлений. Более того, если злоумышленники действуют не слишком грубо, то информационная среда организации может годами быть для них открытой книгой, а организация даже не будет об этом подозревать! И это несмотря на то, что борьба с несанкционированным доступом к конфиденциальной информации не нова, и на поиски ее решения затрачены огромные усилия.

Сегодня становится ясно, что проблема связана не столько с ненадежностью механизмов аутентификации пользователей и управления их правами, встроенных в современные операционные системы, инфраструктурное и прикладное ПО. Главное то, как эти механизмы применяются на практике – в условиях постоянного повышения угроз ИБ и увеличения числа элементов ИС, с которыми пользователь должен взаимодействовать для выполнения своих должностных обязанностей.

Организации реагируют на эти тренды ужесточением корпоративных политик ИБ, требованием использовать уникальные пароли в каждой подсистеме, часто менять их и увеличивать их стойкость. Пользователи же просто не могут удерживать в памяти постоянно меняющиеся и ничего не выражающие длинные последовательности букв и цифр. И стихийно возвращаются к простейшим паролям, а сложные записывают на бумажках. Да и отделы ИБ не в состоянии своевременно перенастраивать вручную механизмы доступа многочисленных прикладных и инфраструктурных элементов ИС при каждом изменении организационного статуса пользователя. Все это воспитывает у сотрудников «ИБ-нигилизм», а в системе ИБ создает бреши, которыми пользуются злоумышленники.

Сегодня подавляющее большинство компьютерных преступлений совершается в обход средств защиты – через инсайдера, имеющего легитимный доступ к нужным данным и поэтому не встречающего сопротивления со стороны системы ИБ. Более того, злоумышленникам, как правило, не нужно вербовать высокопоставленных должностных лиц или внедрять своего агента на второстепенную должность и долго ждать, пока он получит достаточно высокий уровень доверия. Бреши в системе аутентификации, ошибки и задержки в настройке прав доступа позволяют инсайдерам, занимающим второстепенные позиции в организации, получить доступ к нужной информации от имени сотрудника с гораздо более широким кругом полномочий. Именно эти варианты представляют наибольшую опасность для современного предприятия.

Чтобы инвестиции в ИБ вновь стали эффективными, предприятиям надо переосмыслить роль корпоративной системы управления доступом как фундамента всей системы ИБ, привести свою ИБ-стратегию в соответствие с современной парадигмой управления доступом.



ТРИ КИТА КЛАССИЧЕСКОЙ СИСТЕМЫ УПРАВЛЕНИЯ ДОСТУПОМ

Чтобы устранить вышеперечисленные проблемы, ИБ-вендоры разработали три типа специализированных ИБ-решений. Это системы IDM, PKI и SSO.

Система IDM (Identity management) нацелена непосредственно на задачи управления идентификационными данными и правами доступа каждого пользователя ко всем необходимым ему приложениям в корпоративной ИС. IDM-система автоматизирует создание учетных записей во всех информационных системах на основе ролевых моделей доступа, а также поддерживает соответствие фактических прав каждого пользователя ИС его статусу в организации практически в режиме реального времени. Для осуществления этих функций IDM-решение интегрируется как с кадровой системой организации, так и с максимальным числом прикладных ИС.

Как только в кадровой системе фиксируется кадровое событие (прием на работу и увольнение, изменение должности и включение в те или иные временные рабочие группы, пребывание в командировках и отпусках, оформление больничных и др.), IDM-система производит необходимую перенастройку прав доступа пользователя во всех ИТ-системах, с которыми она взаимодействует. Уходят в прошлое ошибки и задержки при отработке ИТ и ИБ отделами заявок кадровой службы, ведь весь процесс полностью автоматизирован.

Кроме того, хорошая IDM-система автоматически проводит аудит всех заведенных учетных записей, выявляя и исправляя необоснованные отклонения в правах доступа. Без системы IDM появление таких отклонений неизбежно, поскольку ошибочное «отсечение» прав не дает пользователю нормально работать и вызывает претензии к службе ИБ, избыточные же права остаются незамеченными. Со временем пользователи обрастают избыточными правами, а в системах подолгу сохраняются активные аккаунты давно уволенных лиц.

Система PKI (Public Key Infrastructure) обеспечивает т. н. двухфакторную аутентификацию пользователей, при которой для доступа к ИТ-приложению нужно не только знать пароль, но и предъявить персональный физический ключ – токен или смарт-карту. Такая технология аутентификации гораздо надежнее традиционных логинов и паролей, ведь физический ключ невозможно подделать, а завладеть им и узнать его ПИН-код гораздо сложнее, чем решить любую из этих задач в отдельности.

Надежность PKI-аутентификации полностью зависит от неукоснительного соблюдения владельцем ключа простых правил, главное из которых – исключить попадание ключа в чужие руки. И хотя это требование очевидно, в реальной жизни оно нарушается достаточно часто – иногда по сговору со злоумышленником, а гораздо чаще из-за банальной халатности. Естественно, в этом случае надежность системы PKI-аутентификации падает до уровня обычных паролей. Именно поэтому в настоящее время основные усилия разработчиков направлены на модернизацию систем аутентификации и перехода от двухфакторной к трехфакторной аутентификации, когда в модель добавляется дополнительный фактор проверки, например, текущее физическое расположение пользователя.

Трехфакторная аутентификация основана на интеграции PKI-инфраструктуры с системой IDM, которая, в свою очередь, взаимодействует с системой контроля физического доступа в помещения (СКУД).

Кроме того, все большее внимание вызывают разработки, обеспечивающие неотчуждаемость ключа от его владельца, в которых применяются биометрические данные и сканеры отпечатков пальцев или радужной оболочки глаза.

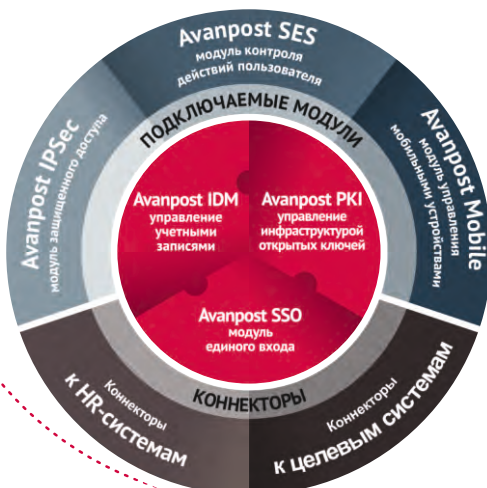
Система SSO (Single Sign-On) устраняет противоречие между классическими канонами безопасности и жесткими требованиями политик ИБ, с одной стороны, и ограниченными возможностями пользователя по запоминанию паролей – с другой. Пользователь один раз проходит аутентификацию с использованием единого идентификатора (ключевого носителя или пароля) – и получает доступ сразу ко всем нужным ему информационным ресурсам. При этом в каждом ресурсе фактически используются очень сложные и стойкие пароли, которые можно обновлять хоть каждый час.

СОВРЕМЕННАЯ ПАРАДИГМА УПРАВЛЕНИЯ ДОСТУПОМ

Без систем IDM, PKI и SSO безошибочное управление доступом невозможно. В то же время, многие российские организации уже внедрили эти системы, но столкнулись с другой проблемой – сложность администрирования большого количества разрозненных систем и механизмов. Т.о., на сегодняшний день наиболее эффективной системой управления доступом является централизованное решение, объединяющее весь необходимый функционал. Только целостная система управления, в которой объединены функции IDM, PKI и SSO, а также средства взаимодействия с удостоверяющими центрами (УЦ), способно решить задачу, не ставя перед организацией новых проблем. Это должны учитывать как предприятия, только приступающие к созданию корпоративной системы управления доступом, так и зрелые организации, широко применяющие двухфакторную аутентификацию на базе токенов.

РЕШЕНИЕ ПК «AVANPOST»

Программный комплекс «Avanpost» представляет собой первый комплексный продукт, автоматизирующий все аспекты, связанные с организацией и управлением доступом к ИТ ресурсам предприятия, и отвечающий требованиям современной парадигмы трех китов IDM, PKI и SSO.



Помимо полной автоматизации задач управления доступом к ИТ-ресурсам предприятия программный комплекс имеет в своем составе дополнительные подключаемые модули – модуль построения защищенных VPN-соединений на базе ГОСТ криптоалгоритмов (IPSec), модуль контроля действий пользователей (SeS), модуль управления мобильными устройствами (Mobile). Функционал каждого из классов систем (IDM, PKI и SSO) выделен в отдельный модуль ПК Avanpost, который способен эффективно работать самостоятельно, без привязки к другим модулям, что позволяет организовывать поэтапное внедрение системы, исходя из потребностей и финансовых возможностей компании-заказчика.

Базовый функционал:

Модуль «Avanpost IDM» предназначен для централизованного управления учетными записями пользователей в различных информационных системах, подключаемых к ПК «Avanpost» посредством коннекторов.

Модуль «Avanpost PKI» предназначен для централизованного управления всеми элементами инфраструктуры открытых ключей (PKI) из единого интерфейса. Сюда входит управление электронными сертификатами, ключевыми носителями, ведение поэкземплярного учета средств криптографической защиты информации (СКЗИ), автоматизация процесса выпуска сертификатов и ведение журналов событий.



Модуль «Avanpost SSO» обеспечивает единый вход в систему или в приложение. При этом пользователи осуществляют вход во все приложения с использованием одного идентификатора, исключая необходимость запоминания множества логинов и паролей, что сокращает время доступа к приложениям.



Три основных модуля системы (IDM, PKI и SSO) работают как единый слаженный комплекс, за счет чего обеспечивается очень высокий уровень автоматизации, информационной безопасности и удобства для клиента, совершенно недостижимый при внедрении систем данных классов, не объединенных в единый программный комплекс.

Другого продукта, объединяющего все три класса в одну систему, на рынке пока не существует!

Подключаемые модули:



«Avanpost IPsec» (Internet security protocol) предназначен для обеспечения конфиденциальности и достоверности потока данных, передаваемых по сети, и авторизации пользователей при доступе к сетевым узлам.



«Avanpost SeS» (Security Supervisor) предназначен для управления доступом сотрудников к автоматизированным рабочим местам и устройствам ввода/вывода информации, входящим в состав корпоративной информационной системы.



«Avanpost Mobile» предназначен для использования собственных мобильных устройств сотрудников для работы с конфиденциальной корпоративной информацией: электронной почтой, хранилищами документов, интранет, различными бизнес-приложениям и др.

Интеграция ПК Avanpost с другими элементами ИС:

Для интеграции решения «Avanpost» в инфраструктуру заказчика используются коннекторы. На текущий момент разработано более 100 коннекторов к самым распространенным ИТ-системам в России. Кроме того, коннекторы разрабатываются самой компанией-разработчиком «Avanpost», что существенно сокращает сроки разработки, а также повышает надежность последующей работы коннектора вне зависимости от воздействия периодических внешних факторов (например, обновление ИТ-системы).



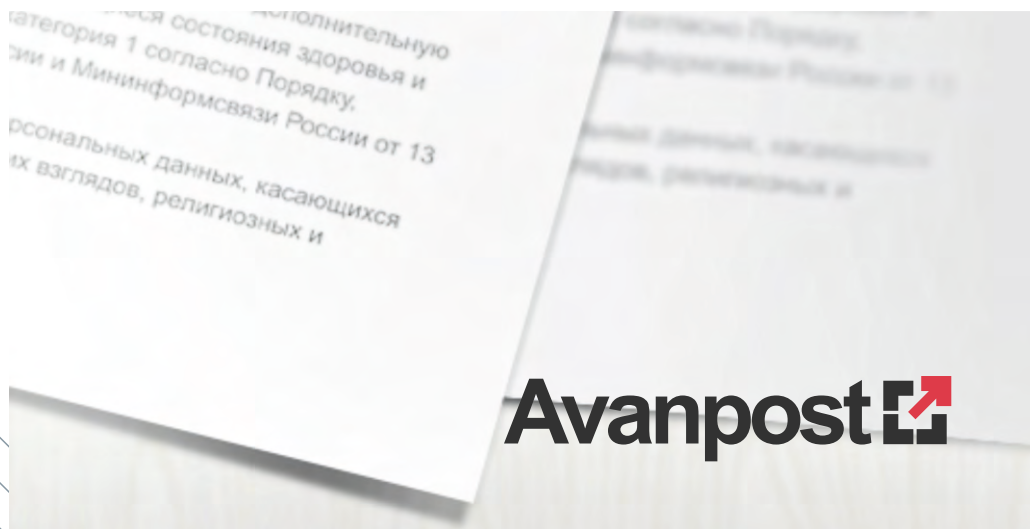
Коннекторы к HR-системам (SAP HR, 1C, Босс-кадровик, Диасофт и др.)



Коннекторы к целевым системам (AD, EPR, CRM, 1C, базы данных и др.)

КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА ПК «AVANPOST»

- 1 Важнейшим преимуществом ПК «Avanpost» является то, что, сочетая в себе функциональность IDM, PKI и SSO, на текущий момент это первое решение, способное полностью автоматизировать все аспекты современной системы управления доступом, при этом обеспечив удобное централизованное администрирование;
- 2 ПК «Avanpost» универсален с точки зрения работы с ключевыми носителями и удостоверяющими центрами. Поддерживается работа с большинством распространенных удостоверяющих центров и криптопровайдеров (КриптоПро, Microsoft, RSA Keon, Signal-COM). Кроме того, ПК «Аванпост» поддерживает подавляющее большинство ключевых носителей различных производителей (вся линейка eToken и JaCarta, вся линейка Rutoken, смарт-карты и т.д.), представленных на территории России. Более того, возможно одновременное использование в организации различных типов ключевых носителей, что разительно отличает «Avanpost» от ряда других систем управления PKI-инфраструктурой, имеющих жесткую привязку к собственным ключевым носителям.
- 3 Поскольку ПК «Аванпост» создавался в России, то одним из принципов разработки было полное соответствие требованиям российского законодательства, отраслевых стандартов и требований регулирующих органов (№152-ФЗ «О персональных данных», СТО БР ИББС, PCI DSS, требования ФСТЭК и ФСБ). Более того, в рамках продукта автоматизирован целый ряд функций, которые значительно облегчают выполнение данных требований. Например, автоматизированный поэкземплярный учет лицензий на средства криптографической защиты информации, требуемый ФСБ.
- 4 Политика лицензирования «Avanpost» такова, что продукт вполне доступен по цене даже для небольших организаций (от 500 пользователей). Это является существенным отличием от крупных западных вендоров, продающих свои системы большими "бандлами", рассчитанными на компании с очень большой численностью персонала.
- 5 Программный комплекс «Avanpost» прошел сертификацию в ФСТЭК России. Сертифицирован по 4 уровню контроля отсутствия недеklarированных возможностей и может быть использован в автоматизированных системах до класса защищенности 1Г включительно и информационных системах персональных данных до 1 класса включительно;
- 6 В настоящее время завершается сертификация программного комплекса в структурах ФСБ России на корректность встраивания криптоалгоритмов (КС2);





- 7 Программный комплекс прост в разворачивании и масштабировании, что делает его эксплуатацию удобной и не требующей дополнительных затрат на длительное обучение персонала.
- 8 Команда разработчиков «Avanpost» находится в России, что существенно облегчает вопросы адаптации продукта под потребности заказчиков. Это особенно актуально для модуля IDM, для эффективной работы которого требуется наличие коннекторов ко всем ИТ-системам, установленным в организации. Практически всегда среди многообразия установленных у клиента ИТ-систем встречаются не очень распространенные или самописные системы, к которым отсутствуют готовые коннекторы у вендоров, предлагающих тяжелые западные IDM-системы (Oracle, IBM, Microsoft). Запросы к таким вендорам с просьбами о разработке коннекторов крайне редко приводят к качественному и оперативному результату. А написание коннекторов силами системных интеграторов, выполняющих внедрение, таит в себе риски нестабильной работы созданных коннекторов, особенно в моменты выхода и установки патчей и новых версий продукта. В случае же с «Avanpost», созданием коннекторов занимается та же команда разработчиков, которая занимается созданием и развитием самого ПК «Avanpost». Такой подход гарантирует стабильную работу коннекторов и отсутствие проблем при выходе новых патчей и версий системы. При этом и сроки, и стоимость разработки коннекторов строго регламентированы и предсказуемы для заказчика;
- 9 Высокий уровень удобства ПК «Avanpost» определяется тем, что у его истоков стояли практики, которые автоматизировали свою собственную деятельность. Первая версия ПК «Avanpost» создавалась как заказная разработка для одного из крупнейших российских банков. Опыт и практика руководителей и специалистов по ИБ, обеспечивающих безопасность огромной организации, работающей не только со своей внутренней информацией, но и с деньгами сотен тысяч клиентов, позволили сделать продукт, в котором очень точно автоматизированы именно те функции и процессы, которыми ежедневно занимаются действующие службы информационной безопасности, а не некоторые научные изыскания аналитиков, оторванных от реальной жизни.

ПЕРСПЕКТИВНЫЕ РАЗРАБОТКИ

Компания Аванпост, как один из признанных технологических лидеров в сегменте систем для эффективного управления доступом, постоянно находится в тесной связи со своими заказчиками и партнерами. Мы постоянно дорабатываем свой программный комплекс, добавляя в него тот функционал, в котором возникает потребность в ходе эксплуатации системы. Кроме того, в настоящее время ведется сразу несколько перспективных разработок, призванных совершить очередной технологический скачок в развитии систем IDM.

«Avanpost» Role Management & Analytics



Role Management & Analytics – новая разработка, призванная существенно упростить создание и управление ролевой моделью на предприятии любого масштаба. Автоматизированный механизм аналитического сравнения существующих прав для пользователей, занимающих одинаковую должность согласно структуре штатного расписания, позволяет сократить время внедрения IDM-системы в 3 раза!

Ни для кого не секрет, что любое внедрение IDM-решения обречено на провал, если в процессе реализации системы не проводится корректное формирование матрицы доступа и ролевой модели.

Именно поэтому практически любому внедрению предшествует достаточно длительный период работ, связанных со сбором и консолидацией инвентаризационной информации о правах доступа пользователей. Затем начинается длительное согласование бизнес-ролей и формирование матрицы доступа. Практика показывает, что данный процесс может растянуться на долгие месяцы, при этом, когда, казалось бы, практически согласован итоговый вариант, получается, что актуальность собранной информации не выдерживает никакой критики. Ведь за время, пока идет анализ и формирование матрицы доступа, этот самый доступ может измениться до неузнаваемости.

Оценив всю серьезность данной проблемы, компания Аванпост начала разработку в рамках модуля Avanpost IDM специализированного инструментария «Avanpost» Role Management & Analytics. Этот инструмент существенно сократит время создания ролевой модели на предприятии любого масштаба. Принцип работы этой надстройки заключается в том, что в процессе развертывания модуля Avanpost IDM сначала производится автоматизированный сбор информации по всем сотрудникам из кадровой подсистемы предприятия, затем производится загрузка всех ролей и привилегий из целевых информационных систем по каждому сотруднику. После этого в консоли аналитической надстройки «Avanpost» Role Management & Analytics администратор системы может запустить первичный процесс создания ролевой модели и уже через несколько минут получить базовую матрицу ролей. Инструмент в автоматическом режиме произведет проверку всех прав доступа по каждой штатной единице и выдаст рекомендации к формированию бизнес ролей.

Проще всего это можно объяснить на следующем примере. Представьте, что в компании в должности главного специалиста отдела продаж работает 10 человек. «Avanpost» Role Management & Analytics проведет сравнение по всем 10 сотрудникам и в результате все те права в ИС, которые у данных сотрудников полностью совпадают, будут рекомендованы как базовые права, присущие бизнес-роли главного специалиста отдела продаж. Если обнаружатся права, которые встречаются, к примеру, у 8 сотрудников из 10, то данные права доступа также будут рекомендованы к включению в бизнес-роль, о чем администратор получит уведомление в диалоговом окне формирования бизнес-ролей. Безусловно, этот инструмент не сможет полностью избавить разработчиков и администраторов от ручной обработки «сложных» случаев, и те права доступа, которые являются уникальными для каждого из 10 рассматриваемых сотрудников, придется в обработать в ручном режиме, отозвав или добавив их в исключения. Но, тем не менее, появление подобного инструмента - это большой шаг вперед в развитии решений класса IDM, и на сегодняшний день ни один производитель решений подобного класса не обладает подобным функционалом.

Плановый срок ввода в промышленную эксплуатацию модуля «Avanpost» Role Management & Analytics намечен на 3 квартал 2013 года.

Развитие модели трехфакторной аутентификации



Трехфакторная аутентификация – развитие модели двухфакторной аутентификации на базе ключевых носителей (токенов или смарт-карт) с применением дополнительной информации для принятия решения о легитимности пользователя. Классически таким дополнительным фактором является информация, получаемая в реальном времени с систем физического контроля доступа СКУД.

В свое время развитие и повсеместное применение модели двухфакторной аутентификации было серьезным шагом вперед в части повышения уровня информационной безопасности в компании. Но практика показала, что одним таким переходом все проблемы ИБ не решить, и нужно проделать огромную работу в первую очередь с пользователями, дабы повысить культуру обращения с ключами и исключить риски компрометации. Пользователи в своей массе либо недостаточно осведомлены, либо не осознают ценность той информации, к которой они имеют доступ, а отсюда следует и халатное обращение с ключевыми носителями, и передача их другим лицам, и банальное оставление токена в компьютере на весь рабочий день. Соответственно, постепенно возникла необходимость модернизации существующей модели и решения проблемы неотчуждаемости ключа от пользователя.

Идея механизма трехфакторной аутентификации на базе ПК «Avanpost» базируется на том, что в рамках принятия решения о допуске / недопуске пользователя в приложение помимо основных факторов (наличие токена и корректного ПИН-кода к нему) в работу вступает еще и третий фактор – физическое месторасположение пользователя. Этот третий фактор корректнее всего получать посредством системы СКУД, т.е., в рамках перспективных разработок и развития продукта ПК «Avanpost» ведется серьезная работа по интеграции решения с самыми распространенными в России системами контроля физического доступа.

Принцип работы такой системы может быть разный. Например, если на предприятии все кабинеты и двери оборудованы считывателями СКУД, можно разрешить пользователю входить в свои корпоративные приложения только в том случае, если он находится в своем кабинете. При этом при попытке входа в ИС, Avanpost в онлайн-режиме будет проверять данные от системы СКУД, и если пользователь согласно информации от СКУД не входил в свой кабинет, то в доступе ему будет отказано. Более того, многие современные ключевые носители (токены и смарт-карты) сегодня могут поставляться со специализированными RFID-метками, используемыми в СКУД, что позволит пользователям применять один и тот же ключ как для доступа в свои корпоративные приложения, так и для перемещения внутри офиса. Это, в свою очередь, автоматически будет означать, что пользователи больше не будут оставлять в компьютерах свои ключи, уходя, к примеру, на обед, ведь иначе они просто не смогут выйти из кабинета или пройти через турникет.

Плановый срок интеграции «Avanpost» с распространенными системами СКУД намечен на 3 квартал 2013 года.

Развитие «Avanpost Mobile»



«Avanpost Mobile» предназначен для использования собственных мобильных устройств сотрудников для работы с конфиденциальной корпоративной информацией: электронной почтой, хранилищами документов, интранет, различными бизнес-приложениями и др.

Сегодня любая компания сталкивается с задачами, связанными с управлением доступом к конфиденциальной информации при помощи мобильных устройств (смартфонов и планшетов). А учитывая постоянно возрастающую ценность конфиденциальной корпоративной информации, эти задачи становятся все более и более актуальными и вызывают головную боль у специалистов ИТ и ИБ-подразделений.

Модуль Avanpost Mobile призван решить эти проблемы, при этом обеспечив удобный и безопасный доступ к корпоративным приложениям всем пользователям использующим мобильные устройства. В настоящее время модуль активно дорабатывается для использования на самых распространенных мобильных платформах: iOS, Android и Windows.

Плановый срок ввода в эксплуатацию полноценного модуля Avanpost Mobile для трех вышеупомянутых платформ – 3 квартал 2013 года.

РЕАЛИЗОВАННЫЕ ПРОЕКТЫ

За последние несколько лет программный комплекс «Avanpost» был успешно внедрен более чем в 50 компаниях кредитно-финансовой, строительной и энергетической отрасли.

Кроме того, были произведены успешные пилотные внедрения более чем на 70 предприятиях самых различных сфер деятельности.

В настоящее время ПК «Avanpost» внедрен и используется в качестве базового элемента системы управления доступом в ряде организаций с территориально распределенной инфраструктурой масштаба всей России (с десятками и даже сотнями тысяч пользователей).

В своих проектах мы всегда готовы идти навстречу заказчику и при необходимости дорабатывать функциональность нашего решения под конкретные потребности. Ниже представлены лишь некоторые наши успешные проекты:



О КОМПАНИИ

Компания Аванпост – ведущий российский разработчик систем идентификации и управления доступом к информационным ресурсам предприятия.

Компания Аванпост является разработчиком программного комплекса «Avanpost» – уникального продукта, по соотношению полноты функционала и стоимости не имеющего аналогов на российском и западном рынках. ПК «Avanpost» позволяет решить задачи, связанные с управлением идентификацией и доступом к информационным ресурсам предприятия (IDM), инфраструктурой открытых ключей (PKI), парольными политиками и аутентификацией (SSO), а также построения защищенных VPN-соединений (IPSec), контроля действий пользователей (SeS) и управления мобильными устройствами (Mobile).

Компания Аванпост работает на рынке информационных технологий и информационной безопасности с июня 2007 года и к настоящему моменту является технологическим лидером в сегменте Identity Management.

С 2012 года компания Аванпост реализует новую модель ведения бизнеса, и перешла на двухэлементную систему распространения, объединяющую использование каналов дистрибуции и партнерства с универсальными-, ИБ- и отраслевыми интеграторами.



КОНТАКТЫ

109316, Москва, Волгоградский пр-т, д.43, корп.3

Тел./факс: +7 (495) 641-80-80

E-mail: info@avanpost.ru

www.avanpost.ru



