БЕЗОПАСНОЕ ОБЛАКО

НАУЧНЫЙ РУКОВОДИТЕЛЬ ФГУП «ВСЕРОССИЙСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ ПРОБЛЕМ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И ИНФОРМАТИЗАЦИИ»
Валерий Аркадьевич Конявский

На одном из заседаний научно-технического совета одного из уважаемых ведомств в выступлении главного конструктора информационных систем прозвучала потрясшая меня метафора. Он описал облачную инфраструктуру как совокупность «облака ЦОДов, облака «серверов доступа» и подключенных к ним сервисов, таких как документооборот, безопасность, почта и других такого же уровня». «Облако ЦОДов» меня потрясло. Я понял, что нужен рассказ, даже не статья, чтобы пояснить основы предметной области, не вдаваясь в конкретику реализации тех или иных принципов.

Ниже я попробую это сделать.

За последние десятилетия мощность компьютеров выросла на многие порядки, человек же, хотя, возможно, и стал умнее, но точно не намного, хотя человечество в целом значительно продвинулось вперед. И, работая на персональных компьютерах, люди используют их возможности совсем незначительно, и чем дальше, тем относительно меньше. Быстродействие мозга не изменилось, оно остается, как и много лет назад, равным приблизительно 50 операциям в секунду. Тактовая частота компьютеров измеряется гигагерцами. Всё, что может человек, – это загрузить компьютер на единицы процентов.

Мы платим за 100% ресурсов компьютера, а используем, например, 2%. В 50 раз переплачиваем. Жалко.

Конечно, если человек будет платить в 5 раз меньше, то ему это выгодно. И если ресурсы компьютера разделить на 20 человек и каждый будет платить за 10% ресурсов, то владелец компьютера останется в ощутимой выгоде, тем более что на оплату энергетики будет уходить в разы меньше средств. Вот такие рассуждения и явились причиной появления систем виртуализации.

На маленьком компьютере можно поддерживать немного виртуальных машин (ВМ). Очевидно, что чем мощнее компьютер, тем больше виртуальных машин может на нем работать и тем эффективнее будет виртуализация. Конечно, в том случае, если большая часть виртуальных машин будет использоваться. Мало их создать, нужно, чтобы они были востребованны.

Если компьютер достаточно мощный и все его ресурсы уже заняты, а виртуальных машин не хватает, тогда нужно покупать еще один компьютер. Станет их много – тогда нужно строить специальное инженерное сооружение, эффективно обеспечивающее энергетикой компьютеры, на которых функционируют ВМ. Всё вместе это называется ЦОД – центр обработки данных. Пользователь знает, на каком ЦОДе размещается его ВМ, но не знает, на каком именно физическом сервере.

Доступ к ВМ для клиента можно организовывать по-разному. Например, если на ВМ установить терминальный сервер, то клиенты могут получать доступ в терминальном режиме. Веб-сервер обеспечит веб-доступ.

Чтобы получить на ЦОДе в свое распоряжение ВМ, нужно определить, какими именно ресурсами эта машина должна располагать, и попросить администратора создать соответствующую ВМ. Однажды созданная ВМ останется именно такой до тех пор, пока не будет изменена или удалена администратором. Другими словами, мы наблюдаем статическое распределение ресурсов. Пользователь знает, где именно находится его ВМ, и что она собой представляет.

Несколько ЦОДов иногда объединяются одним механизмом управления. Теперь ВМ могут размещаться не только на разных физических серверах, но и на разных ЦОДах. Но до сих пор пользователь при желании может точно установить, где находится его конкретная виртуальная машина.

Так может продолжаться до тех пор, пока ресурсов группы ЦОДов хватает для размещения всех требуемых виртуальных машин. Рано или поздно все эти ресурсы окажутся занятыми, и тогда придется «уплотняться».

Мало кто удержится от заказа ВМ «на вырост». Конечно, за заказанные ресурсы нужно платить, но не так много, а значит, лучше взять «про запас». И хотя эффективность использования ресурсов ЦОДа намного выше, чем при использовании ПЭВМ, все-таки оптимальным такое использование не назовешь. Каждый взял себе по 20–30% запаса ресурсов, значит, свободные ресурсы есть, а использовать их нельзя. Неэкономно получается.

Вот только здесь появляется потребность в том, что отличает облако от виртуализации оборудования, – в динамическом распределении (выделении) ресурсов. Облако характеризуется виртуализацией оборудования, виртуализацией ОС, виртуализацией приложений и динамическим распределением ресурсов.

При работе в облаке ВМ может размещаться на любой памяти, исполняться на любом сервере любого ЦОДа, входящего в состав облачной инфраструктуры. Говорят, что ВМ «мигрируют» между ЦОДами. Решение о миграции ВМ принимает «планировщик», исходя из различных соображений, например из логики равномерности загрузки ЦОДа, цены и наличия свободных ресурсов и др. Не принимается во внимание только уровень конфиденциальности информации, обрабатываемой в ВМ.

Таким образом, облачные технологии начинаются тогда, когда исчерпаны все ресурсы ЦОДов, предоставляющих пользователям виртуализированное оборудование на основе использования систем виртуализации. Облачная инфраструктура – это взаимодействующие на основе специализированного планировщика ЦОДы, средства доступа и клиентские машины. Защищенная облачная инфраструктура – это защищенные серверы, защищенные ЦОДы, защищенные ВМ, защищенный доступ (веб- и/или терминальный) и, наконец, защищенный планировщик, планирующий миграцию ВМ из соображений в том числе защищенности информационных ресурсов.

Облако – это всё вместе. Не бывает «облака ЦОДов», «облака серверов доступа», «облака сервисов», бывает облачная инфраструктура в целом и облачные сервисы, скрывающие от пользователя всю эту сложную «механику» и предоставляющие пользователю доступ к тем ресурсам, которые ему нужны.

Важный вопрос: когда же наступает пора перехода на облачную инфраструктуру?

Сначала нужно сделать ЦОД.

Развернуть систему виртуализации оборудования.

Создать виртуальные машины.

Установить на них необходимое программное обеспечение.

Разместить на ЦОДе информационные ресурсы.

Потом подключить к ВМ пользователей.

Дождаться, когда пользователи начнут использовать 70–80% ресурсов.

И только тогда пора думать об облаке.

Здесь опущены вопросы защиты, поскольку не надо создавать защиту облака, не научившись защищать виртуальные машины.

Если сегодня вы используете ресурсы ЦОДа на 0,5% и в ближайший год планируете увеличить эту цифру на порядок, не надо думать об облаке. Например, если в вашем ЦОДе 1 тыс. (это немного) физических серверов и на каждом из них можно поднять 50 (это тоже немного) виртуальных машин, то 50 тыс. (а это уже много) рабочих мест вполне могут поддерживаться и без облака. Вот если на этом ЦОДе вам нужно обеспечить комфортную работу 100 тыс. сотрудников, то пора подумать о планировщике и, соответственно, об организации облачного доступа. Если же в вашей корпорации еще не скоро одновременно будут работать 100 тыс. пользователей или если у вас уже есть ЦОДы, которые могут поддержать достаточное количество ВМ, не надо вам создавать корпоративное облако. Используйте в полной мере ЦОД.

Если же, несмотря ни на что, вы всё же создаете корпоративное облако, то мотивировать вас может только одно: от публичного облака корпоративное отличается защищенностью. В этом смысле строить незащищенное корпоративное облако – задача, вызывающая удивление и у специалистов и у финансовых контролирующих органов.

Дальше поговорим о защите облака.

Облако можно считать защищенным, если как минимум:

- обеспечена доверенная среда на компьютерах пользователей;
- защищен доступ пользователей к ВМ (веб- или терминальный);
- обеспечен контролируемый старт серверов ЦОДа и ВМ на серверах;
- защищены ВМ;
- обеспечена контролируемая миграция ВМ (то есть используется защищенный планировщик).

Эти меры являются необходимыми, но не достаточными, без них говорить о защищенности облачной инфраструктуры нельзя, но они могут сильно расширяться.

Требования к защите облака понятны, ведь если информационное взаимодействие связано с обработкой персональных данных и обработкой государственных информационных ресурсов, то меры по защите должны соответствовать требованиям приказов Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и от 18 февраля 2013 года №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Опишем кратко возможные варианты и средства защиты:

1. *Доверенная среда на компьютерах пользователей* может создаваться применением СЗИ НСД «Аккорд» или СОДС «МАРШ!».

2. *Защищенный доступ пользователей к ВМ* можно обеспечить применением VPN в доверенной среде для веб-доступа или системой доверенной терминальной загрузки «Центр-Т», основанной на применении СКЗИ «ШИПКА».
3. *Контролируемый старт (доверенная загрузка) системы виртуализации* обеспечивается для VMware системой «Аккорд-В.», для MS HV – системой «ГиперАккорд».
4. *Защита ВМ* осуществляется СЗИ НСД «Аккорд-VE» из состава названных выше «Аккорд-В.» или «ГиперАккорд».
5. *Защита планировщика* облака еще находится в разработке.

ДОВЕРЕННАЯ СРЕДА НА КОМПЬЮТЕРАХ ПОЛЬЗОВАТЕЛЕЙ, ИЛИ «СЕРЕБРЯНАЯ ПУЛЯ» ДЛЯ ХАКЕРА

Мы не раз смотрели фильмы и читали книги, в которых борцы с нечистью в конце концов побеждали, применяя различные сакральные инструменты, такие как осиновый кол, чеснок или серебряные пули.

Наша жизнь похожа на эти фильмы – мы тоже сталкиваемся с разными упырями и вампирами, но только от информационных технологий. И многие все-таки «погибают» в этой борьбе. Потом начинается анализ причин.

Было отмечено, что, видимо, «серебряную пулю» создать нельзя. Конечно, это не так. «Серебряная пуля» в технической защите информации существует, и все знают, что это. Просто часто создание доверенной среды информационного взаимодействия подменяют имитацией деятельности, а надежные средства замещают на более дешевые, имитирующие выполнение защитных функций.

Вот несколько примеров очевидно недостоверных идей, которые, однако, высказывались публично и поэтому требуют публичного обсуждения:

– применение токенов обеспечивает достаточный уровень защищенности;
– квалифицированная электронная подпись (ЭП) может быть получена в недоверенной среде;
– если стоит ЭП, то документу можно доверять;
– главный приоритет – удобство клиента, а безопасность – его проблема.

Никакой токен не создает доверенной среды, поэтому первое утверждение недостоверно. В недоверенной среде возможны перехват управления, атака на порты, работа под враждебным гипервизором и т.д. Токен – просто хранилище ключей, которое ничем не лучше, чем дискета, просто токен легче потерять. Неизвлекаемость ключа – полезное свойство, но оно полезно только при доверенности среды, в другом случае – это имитация защиты. Далее будут примеры, подтверждающие этот вывод.

Второе утверждение можно объяснить только дремучей безграмотностью лиц, его придумавших. Недоверенная среда – это «чашка Петри», питательная среда для вирусов и троянов, услужливо посеянных в ней хакерами, готовящимися атаковать ваш компьютер. Не будем даже говорить о том, что требование о доверенности среды прямо связано с требованиями Федерального закона Российской Федерации от 6 апреля 2011 года №63-ФЗ «Об электронной подписи» (далее – ФЗ-63). Наверное, многие тоже пытаются «суровость» закона компенсировать необязательностью его исполнения. Но вот здесь – точно зря!

Утверждение о том, что подпись под файлом делает его документом, – очевидно ложно. Даже если проверка подписи дает правильный результат, это ни о чем не говорит. Правильную подпись хакера под платежкой, отправленной от моего имени, банк не должен считать основанием для платежа. Важны не только результаты проверки подписи, но и полномочия и правомочия подписавшего, а этих полей сегодня нет даже в квалифицированном сертификате.

Четвертый тезис – о приоритете удобства над безопасностью – можно обсудить подробнее. Мне, например, кажется, что безопасность важнее. Хотя я и допускаю, что есть люди, для которых важнее удобство – например потому, что они плохо владеют компьютером. Это вполне весомый аргумент, его не стоит воспринимать с улыбкой. Вспомните, как вы преодолевали первые километры, только получив водительское удостоверение. Было сложно. Но и здесь, хотя особого выбора не было, хотелось управлять безопасным «мерседесом», а не «копейкой».

Личные предпочтения важны, но еще важнее право выбора. Почему кто-то вообще присваивает себе право решать, что лучше для меня? Как нигде важна защита, например, в системах дистанционного банковского обслуживания (ДБО). В этих системах мне предлагают воспользоваться решениями, которые считает достаточными банк. Верю опыту банкиров, но это скорее опыт зарабатывания денег для банка, а не опыт обеспечения безопасности клиента. Это личные предпочтения банкиров, а не забота о клиенте. Мне кажется, что даже из самых благих намерений (которыми, как известно, и вымощена дорога в ад) не нужно навязывать клиенту свои представления о его предпочтениях. Кому-то важно удобство, кому-то безопасность. Полагаю, что клиенту банка должен быть предложен выбор: Дешево, Быстро, Опасно (ДБО) – или Дороже, но БезОпасно (ДБО). Клиент выберет сам, а банк должен предоставить ему возможность выбора, конечно, зарабатывая на этом. Нужно просто в клиентском договоре прописать альтернативу: дешевый токен – и тогда все риски на стороне клиента – или доверенная среда – и тогда за безопасность отвечает банк. Тогда всё будет по-честному.

Таким образом, делаем вывод:

– электронные документы должны подписываться электронной подписью,
– ЭП ставится с помощью средства электронной подписи (СЭП),
– СЭП требует доверенной среды.

С этого момента можно не отвлекаться на поиск решения без доверенной среды. Я бы предложил идеи защиты информационного взаимодействия вне доверенной среды рассматривать наряду с идеями по созданию вечного двигателя – в комиссии по лженауке, а не выносить дискуссию на страницы приличных изданий.

Интуитивно ясно, что такое доверенная среда. Ключевым здесь является слово «доверие». Доверие – это не абсолютная характеристика. Более или менее доверяем мы той или иной декларации – вполне нормальная постановка задачи. Чтобы на этом поле сократить объемы разговоров и спекуляций, регулятор выделил шесть типов нарушителя – от самого простого (например, может случайно сфотографировать экран компьютера на телефон) (Н1) до наиболее квалифицированного и снабженного всеми необходимыми средствами (Н6). Соответственно обозначено разделение средств по этой характеристике – КС1, КС2, КС3, КВ1, КВ2, КА1. Средство, сертифицированное по классу КС1, может успешно противостоять нарушителю Н1, КВ2 – нарушителю Н5. Для понимания градации следует сказать, что нарушитель Н3, по сути, компьютерный недоучка, который только и умеет, что скачать из Интернета программу и запустить ее.

Несмотря на всю размытость (нечеткость) такой классификации, нужно понимать, что в Интернете имеется множество хакерских программ и уж точно много троянов, перехватчиков управления, перехватчиков паролей и других разрушающих программных воздействий. В связи с этим есть ряд мер по защите криптографических средств от несанкционированного доступа (НДС), которые должны быть реализованы обязательно. Среди них:

- обеспечение целостности проверенного программного обеспечения и данных;
- управление доступом пользователя к компьютеру;
- разграничение доступа к программам и данным.

Однако практика показала: создать доверенную среду мало – ее нужно поддерживать в течение всего жизненного цикла. Действительно, если информационная система меняется – а она меняется, – то однажды зафиксированное состояние всегда может измениться, и не в лучшую с точки зрения информационной безопасности сторону. Значит, доверенную среду нужно не только создать, но и поддерживать.

Но как же сделать так, чтобы доверенность среды поддерживалась постоянно?

Заметим, что любое информационное взаимодействие можно представить как взаимодействие клиентов через сервис. Если со стороны сервиса всегда можно обеспечить достаточный уровень квалификации персонала и, соответственно, достаточный уровень информационной безопасности, то обучить всех клиентов всех сервисов, создать приемлемый уровень знаний об информационной безопасности решительно невозможно. Пока не удается даже научить всех грамотно писать и говорить.

Оказывается, что, так как должный уровень квалификации со стороны клиента недостижим в принципе, при организации защиты неквалифицированные действия обязательно создадут «дыру» в защищенности. Очевидно, что делать забор всё выше и выше бессмысленно, пока в заборе остаются дыры. Бессмысленно всё лучше и лучше защищать сервисы, пока «дыра» у клиента.

Что же делать?

Ответ очевиден: средства клиента должны быть ненастраиваемые, а все действия по управлению безопасностью должны быть переданы профессионалам. Простой вывод, но в научный оборот он вводится только сейчас.

А всегда ли клиент какого-либо доверенного сервиса должен работать в доверенной среде? Вряд ли. Это будет слишком высокая цена за удовольствие, например, получить раз в месяц государственную услугу в электронном виде. Скорее, клиенту нужно часто работать в недоверенной среде и лишь иногда организовывать доверенный сеанс связи с доверенным сервисом.

Таким образом, работа в доверенном режиме может осуществляться всё время, а может лишь иногда, в относительно небольшие интервалы времени. В первом случае мы создаем доверенную вычислительную среду (ДВС), во втором – организовываем доверенный сеанс связи (ДСС).

ДВС создается однократно, но стоимость создания относительно велика. Действительно, однажды созданная ДВС должна поддерживаться за счет СЗИ долго, в отдельных случаях – годы. За это время суммарное количество атак может стать огромным, и все эти атаки должны быть отражены защитными механизмами СЗИ. Конечно, такие СЗИ стоят дорого.

ДСС создается каждый раз заново, и это в ряде случаев может быть неудобно, ведь загрузка и проверочные мероприятия продолжаются 30–50 секунд, но средства ДСС стоят гораздо дешевле, так как длительность ДСС не всегда достигает и 20 минут.

Вот в этом и состоит основная идея доверенного сеанса связи и его отличие от традиционного подхода. С этим связана и методика выбора: если вы все время должны быть в доверенной среде – создавайте и поддерживайте ДВС. Если доверенность нужна лишь иногда – достаточно и удобнее применять ДСС.

Для этого случая нужно предложить устройство, с которого могла бы осуществляться загрузка, оно было бы отчуждаемым и не теряло бы своих свойств при атаках.

Хорошим вариантом является USB-устройство. Конечно, оно должно быть не простой памятью, ведь если память устройства находится в адресном пространстве компьютера, это устройство не может выполнять функции защиты.

Специализированное устройство получило название «МАРШ!».

Конструктивно «МАРШ!» выполнен в виде USB-устройства и выглядит точно так же, как обычный флеш-накопитель. Такой конструктив позволяет использовать «МАРШ!» практически со всеми компьютерами, так как почти все компьютеры имеют достаточное количество портов USB.

Тем не менее «МАРШ!» похож на флешку только внешне. На самом деле это активное микропроцессорное устройство, с многоконтурной криптографической подсистемой, проверенной защищенной операционной системой Linux, браузером, специальной подсистемой управления к памяти и многим другим.

Основная задача устройства – создание доверенной среды функционирования криптографии. Для этого в специальном разделе его памяти размещается всё необходимое для этого программное обеспечение. Важнейшей

особенностью является обеспечиваемая этим устройством возможность подписи документов в формате XML.

«МАРШ!» подготавливается к эксплуатации как загрузочное устройство. При начале доверенного сеанса связи пользователь загружается с него, обеспечивая тем самым доверенную среду. Далее стартует браузер и всё сопутствующее программное обеспечение, необходимое для работы. В браузере в доверенном сеансе обеспечивается защищенный обмен информацией, с соблюдением всех требований ФЗ-63.

Загрузка производится из защищенной от записи памяти, жесткий диск компьютера не используется. Конфигурация загруженной операционной системы максимально ограничивает свободу пользователя: ему недоступны органы управления операционной системы, рабочая среда полностью изолирована от посторонних сетевых соединений, открытый трафик отсутствует, после завершения работы в браузере сеанс связи завершается, не давая пользователю делать лишнего.

После загрузки операционной системы на компьютер клиента и старта браузера устанавливается доверенный сеанс связи с сервером (VPN-шлюзом) центральной информационной системы (ИС), то есть защищенное соединение на основе криптографических алгоритмов (закрытые ключи и сертификаты хранятся в защищенной памяти устройства «МАРШ!»). Сервер ИС выполняет авторизацию пользователя на доступ к сервисам ИС и соединение с требуемым сервисом.

Способ реализации ДСС за счет динамического формирования доверенной вычислительной среды инвариантен относительно используемых технологий и конфигураций средств вычислительной техники и расширяет общепринятый подход к обеспечению безопасности информации. Исчезает также «привязанность» пользователя и средств обеспечения информационной безопасности к конкретной рабочей станции.

Почему же «МАРШ!» – это «серебряная пуля» для хакера?

Потому что:

- состояние критичных компонентов зафиксировано,
- вирусы блокированы,
- ключи неизвлекаемые,
- перехват управления невозможен,
- управление безопасностью отчуждено от клиента.

Очевидно, что не во всех без исключения случаях целесообразно защищать клиентские рабочие места только с помощью «МАРШ!».

В этом смысле необходимо учитывать два обстоятельства:

1) являются ли пользовательские рабочие места контролируемыми (это так, если ЦОД корпоративный и пользователи – сотрудники организации, но не так, если это ЦОД, предоставляющий облачные сервисы неограниченному кругу пользователей, использующих неограниченный круг компьютеров);
2) ПЭВМ или тонкие клиенты используются в качестве рабочих мест пользователей.

Легко заметить, что эти вопросы находятся в иерархической связи и дают следующие варианты систем:

1. Фиксированные рабочие места пользователей, контролируемые (управляемые) службой информационной безопасности (относится она к владельцу ЦОДа или нет – вопрос в данном случае второстепенный, достаточно знать, что какой-то службой информационной безопасности рабочие места контролируются):
   - ПЭВМ,
   - тонкие клиенты.
2. Неизвестный и неконтролируемый парк СВТ.

Очевидно, что «МАРШ!» – это единственный приемлемый вариант для случая с неизвестным и неконтролируемым парком клиентских мест.

Столь же очевидно, что в случае, когда рабочие места фиксированные, контролируются службой безопасности и представляют собой ПЭВМ, почти наверняка они используются не только для взаимодействия с ЦОДом, но и автономно. И значит, они должны быть защищены полноценным программно-аппаратным комплексом СЗИ НСД (например, «Аккорд-Win32» или «Аккорд-Win64», в зависимости от разрядности ОС на этих ПЭВМ). В зависимости от политики безопасности запуск ВМ может требовать от пользователя подключения, например, другого идентификатора.

Важно понимать, что даже в том случае, если единственной задачей пользователя ПЭВМ является работа с виртуальной инфраструктурой, всё равно необходима установка именно ПАК. Ограничиваться только «Аккордом-АМДЗ» – неверно, так как даже если пользователь не должен, он может использовать ОС своего компьютера для каких-либо не поставленных перед ним задач, и необходимо контролировать потенциальный общий ресурс.

Применение тонких клиентов, как правило, связано с тем, что локально задачи пользователями не выполняются или они минимальны. В то же время ОС тонких клиентов тоже должна быть доверенной. И в этом случае целесообразно применять либо «МАРШ!», либо – если пользователи работают в терминальном режиме с виртуальным терминальным сервером – ПАК «Центр-Т», обеспечивающий защищенное хранение и доверенную сетевую загрузку образов ПО терминальных станций с подтверждением их целостности и аутентичности.

Применение «Центр-Т» удобно в тех случаях, когда актуальна задача обновлений и другого рода модификаций образов терминальных станций без приостановки эксплуатации системы в штатном режиме. На специальном АРМ «Центр» (он реализован на ПСКЗИ «ШИПКА» и загружается на произвольный ПК, не оставляя на нем после отключения СКЗИ никаких следов) администратор редактирует образы ОС, вырабатывает коды аутентификации (КА) для контроля их целостности и аутентичности, записывает их на другое СКЗИ, с которого загружается на произвольный ПК «Сервер хранения и сетевой загрузки», а оттуда, в свою очередь, их получают по сети клиентские СКЗИ и загружают после проверки КА. За счет того, что целостность и аутентичность образов контролируются с помощью

КА, а не контрольных сумм, и достигается ключевой эффект – защищенное обновление образов без организационных сложностей и остановки работы.

При этом с точки зрения действий пользователей система практически не будет отличаться, с одной стороны, от построенной на базе «МАРШ!», а с другой – от «реальной» терминальной системы: пользователь будет подключать USB-устройство, вводить PIN-код и ожидать загрузки терминала и старта сессии с терминальным сервером. Что он виртуальный, пользователь может и вовсе не знать. В рамках сессии то же USB-устройство выполняет функцию идентификатора пользователя в ПАК СЗИ НСД на серверной части системы.

КОНТРОЛИРУЕМЫЙ СТАРТ СИСТЕМЫ ВИРТУАЛИЗАЦИИ, ЗАЩИТА ВМ

ЦОДы могут быть с виртуализацией на базе VMware или на базе Hyper-V.

Рассмотрим защиту инфраструктуры на базе VMware на примере ПАК «Аккорд-В.».

«Аккорд-В.» обеспечивает защиту всех компонентов среды виртуализации: ESXi-серверов и самих виртуальных машин, серверов управления vCenter и дополнительных серверов со службами VMware (например, VMware Consolidated Backup).

Система защиты «Аккорд-В.» полностью интегрируется в инфраструктуру виртуализации, поэтому для ее функционирования не требуются дополнительные серверы. При этом «Аккорд-В.» не ограничивает в целях безопасности возможностей виртуальной инфраструктуры, оставляя доступными все ее преимущества.

В «Аккорд-В.» реализованы следующие механизмы защиты:

- доверенная загрузка всех элементов инфраструктуры виртуализации;
- пошаговый контроль целостности гипервизора, виртуальных машин, файлов внутри виртуальных машин и серверов управления инфраструктурой;
- разграничение доступа администраторов виртуальной инфраструктуры и администраторов безопасности;
- разграничение доступа пользователей внутри виртуальных машин;
- аппаратная идентификация всех пользователей и администраторов инфраструктуры виртуализации.

Управление системой защиты осуществляется централизованно с сервера управления виртуальной инфраструктурой. Доступ к инструментам управления системой защиты предоставляется только администраторам безопасности, от администраторов виртуальной инфраструктуры эти инструменты скрыты.

Защиту инфраструктуры на базе Hyper-V рассмотрим на примере ПАК «ГиперАккорд».

Интерфейс управления комплекса аналогичен ПАК «Аккорд-Win32» и «Аккорд-Win64», поэтому необходимость переучивания управляющего персонала минимальна.

В «ГиперАккорд» реализованы следующие механизмы защиты:

- идентификация/аутентификация пользователей до загрузки ОС;
- проверка целостности критичных для работы службы Hyper-V программ, данных и ветвей реестра до загрузки ОС;
- аутентификация администраторов виртуальной инфраструктуры и администраторов информационной безопасности;
- разграничение доступа пользователей к серверу Windows 2008;
- разграничение доступа к файлам и данным службы Hyper-V;
- разграничение доступа к виртуальным или физическим дискам виртуальных машин;
- защита средств управления виртуальной инфраструктурой от НСД;
- контроль запуска виртуальных машин;
- контроль целостности конфигурации виртуальных машин;
- контроль целостности файлов и данных виртуальных машин (виртуальных дисков);
- доверенная загрузка виртуальных машин.

Для обеспечения полноценной защиты виртуальных машин от НСД рекомендуется на виртуальных машинах использовать ПАК «Аккорд-Win32», «Аккорд-Win64» или «Аккорд-X».

Комплекс работает на всех версиях Hyper-V (версии 2 и 3 для Windows 2008 R2 и 2012 соответственно).

Таким образом, обеспечивается громадный рынок защищенных коммуникаций. Для поддержки этих решений в клиентский компьютер встраивается агент СЗИ НСД «Аккорд» и ПО, поддерживающее необходимые протоколы доступа, включая работу в терминальном режиме и режиме веб-доступа.