Все, что вам следует знать об МЗ АРМ "БДМ"

Екатерина Андреева, *менеджер продукта, АО "ЭЛВИС-ПЛЮС"*

Не секрет, что за последнюю пару лет резко возрос процент работников, сидящих на удаленке. Если ранее мобильными рабочими местами пользовались в основном только сотрудники, выезжающие в командировку или проводящие выездные мероприятия, то уже с 2020 года ввиду объективных причин возможность уйти на дистанционную работу стала необходимостью для большинства офисных работников. Плюсы такой мобильности очевидны: в любой момент можно подключиться к корпоративной среде, просмотреть почту, ответить на письма, отправить документы, даже обсудить важные вопросы на совещании по аудио- и видеосвязи. И все это — не приезжая в офис.

Однако в то же время становится актуальным вопрос защиты такого мобильного рабочего места от различных угроз, возникающих ввиду специфики удаленного подключения. Это и угрозы потери и хищения устройства с важными данными, и вероятность заражения вредоносным ПО, и возможный перехват сетевого трафика при подключении к корпоративным информационным системам через небезопасные точки доступа.

Что же, отвергнуть мобильность как небезопасный способ? Такое решение вряд ли реально: значимость удаленной работы, как показала практика, высока, особенно в условиях пандемии, когда требуется обеспечить непрерывность производственных процессов.

Может быть, попытаться закрыть известные угрозы? А вот этот путь как раз правильный, и он безальтернативен, особенно если мобильные пользователи подключаются к таким системам, как ИСПДн, ГИС, ОКИИ.

Технологии, которые могут обеспечить закрытие перечисленных угроз, известны:

- защита загрузки устройства: чтобы никто, кроме самого пользователя, не смог получить доступ к информации, хранящейся на мобильном устройстве;
- использование доверенной среды функционирования: чтобы быть уверенным, что программная и аппаратная среда мобильного устройства никоим образом не изменилась;
- шифрование: чтобы информация с устройства, даже попав в чужие руки, не могла быть прочитана или перехвачена в сеансе связи.

Данные технологии реализуются различными видами программного и аппаратного обеспечения. Например, защиту загрузки устройства можно обеспечить аппаратно-программным модулем доверенной загрузки (АПМДЗ), однако тут же возникают вопросы. Как этот модуль установить под кожух небольшого устройства? Как весь этот процесс внедрить в производственную линию, сохранив баланс качества и скорости создания партии таких устройств (ведь пользователю устройство обычно нужно "еще вчера")?

Необходимо, чтобы АПМДЗ контролировал неизменность аппаратной и программной среды, обеспечивал шифрование канала связи, а также непосредственно шифровал диск устройства. Но на практике реализация такого функционала потребует целый набор специализированного ПО, а работа пользователя на этом устройстве вполне может превратиться в мучение.

Кроме того, затруднено обслуживание таких платформ для администраторов информационных систем, поскольку каждый компонент обычно устанавливается на аппаратную платформу по своим правилам. Вопрос обслуживания такого набора компонентов не был бы столь болезненным, если бы в компании было от силы 30–50 мобильных пользователей, но что делать, если их должно быть пятьсот, тысяча, две тысячи, и все разбросаны по разным уголкам страны?

Решение есть

Очевидно, что наиболее привлекательным кажется решение, которое совмещало бы в себе все технологии, а процесс его развертывания не был бы сложным и трудоемким.

Таким решением является СКЗИ "Мобильное защищенное автоматизированное рабочее место "Базовый Доверенный Модуль" производства АО "ЭЛВИС-ПЛЮС", обеспечивающее:

- доверенную загрузку ОС;
- контроль целостности аппаратной и программной частей платформы;
- двухфакторную аутентификацию пользователя до загрузки ОС;
- прозрачное шифрование диска в режиме реального времени без влияния на работу пользователя.

Шифрование канала связи обеспечивается ПК "ЗАСТАВА-Клиент" (сертификаты ФСБ России СФ/114-4115 от 30.06.2021 г. и ФСТЭК России № 4249 от 19.05.2020 г.) также производства АО "ЭЛВИС-ПЛЮС". В расширенном варианте поставки в доверенную среду могут добавляться средства защиты информации, уже использующиеся заказчиком.

СКЗИ "МЗ АРМ "БДМ" не требует установки каких-либо аппаратных замков, плат расширения и прочих дополнительных модулей. Развертывание такого решения даже на 2–3 тыс. устройств не займет много времени, поскольку доверенная среда подготавливается заранее, а процесс установки заключается во вводе 2–3 команд.

СКЗИ "МЗ АРМ "БДМ" является сертифицированным средством криптографической защиты информации класса КС1 (сертификат ФСБ России СФ/114-4050 от 07.04.2021 г.).

Больше информации об СКЗИ "МЗ АРМ "БДМ" можно найти на сайте www.elvis.ru.

По вопросам приобретения СКЗИ "МЗ АРМ "БДМ" обращайтесь в дирекцию продаж АО "ЭЛВИС-ПЛЮС" по телефону +7 (495) 276-0211 или электронной почте presale@elvis.ru. ●