В.А. Мельников, асп.; рук. В.И. Луканина, к.т.н., доц. (МЭИ (ТУ))

МОДЕЛЬ ДОСТУПА К РАБОЧИМ СТАНЦИЯМ ПРИ УДАЛЁННОМ АДМИНИСТРИРОВАНИИ

В настоящее время производители программного обеспечения для удалённого администрирования уделяют недостаточно внимания контролю действий системных администраторов на обслуживаемых машинах. Недобросовестный сотрудник с правами администратора может выполнить любые действия на удалённой машине и изменить лог-файл так, что будет невозможно отличить действия администратора от действий пользователя. Так же администратор может отрицать факт доступа к удалённой машине.

Научная новизна работы заключается в том, что предлагается модель доступа, при которой уполномоченный сотрудник не сможет отрицать факт доступа к удалённой машине.

Полученные результаты можно использовать для проектирования систем удалённого администрирования в любых локальных вычислительных сетях [1], независимо от используемых операционных систем.

Основные положения предлагаемой модели:

- никому не доступен пароль для получения доступа к удалённой машине;

- пароль для доступа к удалённой машине генерируется после аутентификации администратора;

- после осуществления доступа к удалённой машине воспользоваться предыдущим паролем невозможно;

- решение о предоставлении доступа администратору осуществляется специальным сервером;

- для защиты от получения пароля злоумышленником и подмены сервера аутентификации используется асимметричная криптография [2];

- данные о действиях администраторов хранятся на специальном сервере.

При применении предлагаемой модели можно выделить следующие преимущества:

- централизация управления учетными записями администраторов;

- все попытки получить удалённый доступ фиксируются агентом, независимо от прав доступа администратора;

- отпадает необходимость помнить пароли от всех администрируемых рабочих станций;

- атака на хеш пароля становится неактуальной;

- подмена агента, не зная его закрытого ключа, не принесёт результатов.

Литература

1. **Banerjee R.,** Internetworking Technologies. Prentice-Hall of India, 2002

2. **Бернет С., Пэйн С.,** Криптография. Изд.: Бином-пресс, 2009