```
5                                   if (!RAND_load_file("/dev/urandom",
                                seedbytes)) {
6                                       return -1;
7                                   }
8                                   opensslIsSeeded = 1;
9                       }
10                                  if      (!RAND_bytes((unsigned      char
                                *)cKeyBuffer, KEYSIZE )) {
11                      }
```

ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМЫ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ КОРПОРАТИВНОЙ СЕТИ ПРЕДПРИЯТИЯ

П.А. Домино, С.Н. Петров

Сегодня число программных продуктов, используемых в любой компании, довольно велико. Также существует тенденция увеличения их количества, причем независимо от профиля компании.

Информация и технологии ее обработки играют ключевую роль в эффективном функционировании и управлении предприятием. Имея доступ к нужной информации — технологической, кадровой, маркетинговой или финансовой, — можно правильно оценить текущую ситуацию, принять своевременные решения. В то же время информация должна быть доступна только тем, кому она предназначена, и скрыта от сторонних наблюдателей.

Известно, что более 25% злоупотреблений информацией в информационных сетях совершаются внутренними пользователями, партнерами и поставщиками услуг, имеющими прямой доступ к сети. До 70% из них — случаи несанкционированного получения прав и привилегий, кражи и передачи учетной информации пользователей сети предприятия, что становится возможным из-за несовершенства технологий разграничения доступа и аутентификации пользователей. Совершенствование методов системы управления доступом и регистрации пользователей является одним из приоритетных направлений развития информационной сети предприятия. Аутентификация является обязательной частью управления доступом в сетях предприятий, без нее нет возможности ограничить доступ пользователей к конкретным информационным ресурсами.

Проведены обзор существующих механизмов аутентификации и сравнение на основе таких показателей, как надёжность и безопасность, эффективность, а так же затраты на установку и обслуживание.

Затраты на обслуживание и эффективность определялись как время, затраченное администратором системы, на ее установку и обслуживание, а также время, затраченное пользователем системы, для прохождения процедуры аутентификации.

Также учитывались финансовые затраты на установку системы, ее обслуживание, а также затраты злоумышленника, требуемые для успешного прохождения аутентификации с помощью определённого типа атаки. В качестве атаки по умолчанию рассматривалась атака методом грубой силы.

ШИФРОВАНИЕ ДАННЫХ С ХАОТИЧЕСКИМИ ИЗМЕНЕНИЯМИ РАУНДОВОГО КЛЮЧА НА ОСНОВЕ ДИНАМИЧЕСКОГО ХАОСА

Д.А. Жуковец

Большинство блочных алгоритмов шифрования одинаково шифруют блоки исходного текста. При этом, если исходное изображение черного цвета, то при шифровании получаем последовательность одинаковых зашифрованных блоков. Чтобы исключить это, в алгоритмах при шифровании используются режимы шифрования CBC, CFB и другие. Однако в режиме CBC (режиме сцепления блоков) при изменении одного бита в исходном тексте при наличии лавинного эффекта могут произойти не только вариации в зашифрованном изображении, но и неполное восстановление исходной информации.

Предлагаемый способ шифрования данных с хаотическими изменениями раундового ключа на основе динамического хаоса позволяет не только увеличить степень защищенности информации, но и обеспечить эффективность шифрования путем повышения стойкости алгоритма шифрования.