```
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.

Литература

1. A novel block encryption scheme based on chaos and an S-box for wireless sensor networks / Tong Xiao-Jun, Wang Zhu, Zuo Ke // Chin. Phys. B Vol. 21, No. 2(2012), URL: http://cpb.iphy.ac.cn/fileup/PDF/2012-2-020506.pdf

СИСТЕМА ЗАЩИТЫ WEB-ПРИЛОЖЕНИЯ НА ОСНОВЕ АСПЕКТНО-ОРИЕНТИРОВАННОГО ПРОГРАММИРОВАНИЯ

С.А. Зайкова, О.Ю. Рыжко

Одним из основных требований, предъявляемых к современным информационным ресурсам и сервисам, является их широкая доступность. Наиболее активное развитие получили web-приложения, в которых роль клиента играет браузер, а роль сервера — web-сервер. В связи с этим встает вопрос об организации разграничения доступа и защите информации. Современные web-приложения имеют многослойную структуру и сложность кода, порой, возрастающего в геометрической прогрессии. Отдельные модули приложений разрабатываются разными командами, которые могут знать о другом модуле только его интерфейс. Актуальность исследования вытекает из необходимости выработки методов выделения функционала обеспечения безопасности web-приложения в отдельный независимый модуль, с возможностью повторного использования кода в совместимых проектах. Это позволит изменять политики безопасности web-приложения централизованно и без изменения бизнес-логики проекта. Проблематика заключается в тесной интеграции инструментов аспектно-ориентированного программирования с кодом целевого web-приложения, сложности внедрения аспектно-ориентированного программирования в проект, а также большом влиянии аспектов на производительность web-приложения, что, в свою очередь, зависит от типа внедрения аспектов и архитектуры приложения. Как показало исследование, использование annotation-driven подхода при разработке, а также конфигурация web-приложения через xml файлы позволяет значительно сократить объем кода приложения, но может вызвать дополнительные временные затраты на отладку и проверку совместимости зависимых библиотек. Разработанная система безопасности является проектно-независимой и может быть применена в другом web-приложении, при условии совместимости интерфейсов в контрактном программировании.

Литература

1. *Safonov V.O.* Using aspect-oriented programming for trustworthy software development — Wiley Interscience: John Wiley & Sons, 2008. — 338 с.

СЛУЧАЙНЫЕ ПРОСТРАНСТВЕННО-ВРЕМЕННЫЕ КОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В ШИРОКОВЕЩАТЕЛЬНЫХ КАНАЛАХ

Т.М. Казубович, С.Б. Саломатин

Современные системы связи и беспроводного доступа широко используют широковещательные многолучевые каналы передачи информации. При этом актуальной является задача защиты каналов связи от подслушивания.

Один из методов решения такой задачи основан на применении технологии MIMO с обратной связью и случайного пространственно-временного кодирования.

Технология MIMO позволяет осуществить эффективный прием информации в условиях многолучевого распространения сигнала за счет создания пространственно-временной избыточности на приемной и передающих сторонах и измерения характеристик канала. Предполагается, что многолучевые каналы имеют существенные различия в разных точках приема. Передающая сторона имеет информацию о состоянии канала связи H с авторизованным пользователем. Подслушивающая сторона такой информации не имеет и вынуждена использовать методы слепой оценки многолучевого канала.

Для защиты информации передающая сторона случайным образом выбирает веса W антенной системы с условием выполнения равенства HW = A, где A — диагональная матрица с положительными диагональными элементами. Авторизованный пользователь принимает сигнал y = HWx + n, где n — вектор шума. Оценивая мощность принятого сигнала, и вычисляя обратную к A матрицу Ai, авторизованный пользователь детектирует информацию x = Ai.y. Случайная весовая матрица пространственно-временного кода имеет две составляющих. Одна составляющая выбирается из условия нормальной рандомизации вектора передаваемого сообщения, а вторая составляющая учитывает информацию о состояния канала.