Все заботы о выборе алгоритма и особенностях аутентификации теперь лежат на PAM. Формально PAM выполнен в виде разделяемых библиотек-модулей, комфортно расположившихся в каталоге /lib/security/. Каждый модуль по-особому пропускает через себя пользователя, реализуя свой особенный механизм аутентификации. Сценарии авторизации находятся в каталоге /etc/pam.d. Имя каждого сценария в этом каталоге совпадает с именем программы, для которого он предназначен. Например, сценарий для login находится по адресу /etc/pam.d/login [4].

Модуль USB, который может быть использован для двухфакторной авторизации, разрабатывается отдельно от основного приложения PAM и пока считается незавершенным, хотя на самом деле полностью функционален. Называется он Pam_usb, и его можно найти на сайте разработчиков [5]. Последняя версия работает с ядрами 2.6 и современными дистрибутивами [5, 6].

Однако модуль Pam_usb по сути реализует стандартную схему «логин/пароль» [5, 6]. Реализовывать стандартную схему не имеет смысла. Поэтому можно придумать нечто новое. Назовем этот модуль pam_enigma.so. Будем спрашивать у пользователя загадки: правильный ответ позволит войти в систему, а ошибочный запросит стандартный пароль при соответствующей настройке стека модулей PAM. База загадок и отгадок будет храниться непосредственно в модуле (хотя возможно настроить и отдельное хранение). Загадки выбираются случайным образом. После написания и сборки модуля скопируем файл pam_enigma.so в /lib/security/ и добавим соответствующую запись в стек модулей PAM. Пример использования модуля приведен ниже:

sasha$su test

Что это такое: синий, большой, с усами и полностью набит зайцами?

троллейбус

test$

Таким образом, в работе рассмотрена возможность создания средств двухфакторной авторизации для операционной системы Linux. Кроме того, рассмотрен вариант замены стандартной авторизации типа «логин/пароль».

СПИСОК ЛИТЕРАТУРЫ:

1. *Малюк А. А., Пазизин С. В., Погожин Н. С.* Введение в защиту информации в автоматизированных системах. М.: Горячая линия — Телеком, 2001. — 148 с.
2. Secret Net. Продукты компании Код безопасности. URL: http://www.securitycode.ru/products/secret_net (дата обращения: 18.11.2009).
3. Aladdin: краткое описание eToken. URL: http://www.aladdin.ru/catalog/etoken/etoken.php (дата обращения: 18.11.2009).
4. Начала PAM // Linux SoftWare Library — Российский портал Linux программ. URL: http://www.linuxsoft.ru/info/lib/lib/secur/pam.htm (дата обращения: 18.11.2009).
5. PAM-usb. URL: http://www.pamusb.org (дата обращения: 18.11.2009).
6. Linux PAM. URL: http://www.kernel.org/pub/linux/libs/pam/ (дата обращения: 18.11.2009).

Д. Ю. Персанов

МЕНЕДЖМЕНТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В работе освещены вопросы управления инцидентами информационной безопасности на предприятии. Рассмотрены аспекты классификации событий и инцидентов информационной безопасности.

Представлена схема процесса мониторинга и обработки событий информационной безопасности. Освещен ряд критичных точек процесса, предложены практические рекомендации по внедрению нового и оптимизации существующих процессов на предприятии.

1. Понятия события и инцидента информационной безопасности.

2. Возможная классификация событий информационной безопасности как инцидентов.

3. Роль инцидентного сервиса в Системе менеджмента информационной безопасности предприятия.

4. Распределение ролей персонала в процессе менеджмента инцидентов ИБ.

5. Процесс менеджмента событий ИБ. Формализация процесса.

6. Критические точки процесса.

7. Важность вопросов применения менеджмента инцидентов ИБ с точки зрения оптимизации расходов предприятия на собственную безопасность.

8. Практические рекомендации по внедрению процесса менеджмента инцидентов ИБ на предприятии.

9. Практические рекомендации по оптимизации существующих процессов.

СПИСОК ЛИТЕРАТУРЫ:

1. Международный стандарт ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования.
2. Служебная процедура ООО «ИБС ДатаФорт» ПР-24 «Управление инцидентами».
3. Служебная процедура ООО «ИБС ДатаФорт» ПР-25 «Мониторинг и обработка событий информационной безопасности».
4. Служебная процедура ООО «ИБС ДатаФорт» ПР-32 «Жизненный цикл запросов и инцидентов».

П. С. Полищук

ПОВЫШЕНИЕ УРОВНЯ ЗАЩИЩЕННОСТИ ПРИ РАБОТЕ С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ, ИСПОЛЬЗУЮЩИМ OPENMP

В работе рассматривается вычислительная среда, к которой могут свободно подключаться различные пользователи с целью запуска своих программных приложений или предоставления в аренду вычислительных ресурсов на коммерческой основе. Для обеспечения безопасности в таких условиях требуется верификация кода, запускаемого пользователями. Приводится метод, позволяющий повысить безопасность подобной среды при работе с приложениями, использующими OpenMP, при этом не затрачивая большое количество ресурсов на процесс верификации.

Рассматривается модель нарушителя. Всех пользователей среды условно можно разделить на три группы: пользователи с правами администратора, пользователи с правами на запуск программного обеспечения и пользователи без прав на запуск программного обеспечения [1]. На этой основе можно выделить три типа угроз: угрозы, возникающие в результате злонамеренного изменения настроек сети администратором; угрозы, исходящие непосредственно от вредоносного программного обеспечения, и угрозы, возникающие в результате манипуляций с ресурсами их владельцев. В работе рассматриваются только те из угроз, которые имеют отношение к