

# УНИВЕРСАЛЬНЫЙ ДИСТРИБУТИВ GNU/LINUX

## НАДЕЖНОСТЬ

Надежная и безопасная платформа для ваших приложений

## ГИБКОСТЬ

Широчайший выбор программ для использования

## УДОБСТВО

Удобства при установке, настройке и работе



## ПРЕДПРИЯТИЯМ

Универсальная и надежная серверная платформа

## РАЗРАБОТЧИКАМ

Широкий выбор средств разработки для различных языков программирования

## ПОЛЬЗОВАТЕЛЯМ

Разнообразные графические среды, офисные и мультимедийные приложения

ALT Linux Master - универсальный дистрибутив GNU/Linux, предназначенный для использования как на серверах, так и на рабочих станциях разработчиков и пользователей.

При подготовке дистрибутива, мы постарались обеспечить максимальную надежность, удобство работы пользователей и безопасность системы.

[www.altlinux.ru](http://www.altlinux.ru)

Москва, ул. Волхонка, 14, оф. 519  
+7 (095) 203-9698

системный администратор

№1(14) январь 2004

подписной индекс 81655

# СИСТЕМНЫЙ АДМИНИСТРАТОР

журнал для системных администраторов,  
вебмастеров и программистов

Вирусы в UNIX, или Гибель  
«Титаника» II

Безопасность  
беспроводных сетей

Защита от хакерских атак  
с помощью ipfw

Как бороться с rootkits

RSBAC для Linux

Active Directory – теория  
построения

Эффективная работа  
с портами в FreeBSD

Безопасность услуг  
хостинга

№1(14) январь 2004



## КАЛЕНДАРЬ СОБЫТИЙ

## Итоги SYSM.02 2

## БЕЗОПАСНОСТЬ

## Вирусы в UNIX, или Гибель «Титаника» II

Способы обнаружения вирусов. Средства защиты.

**Крис Касперски**  
 kk@sendmail.ru 6

## Что такое rootkits, и как с ними бороться

Современный вариант троянского коня: набор утилит rootkits. Как защититься?

**Сергей Яремчук**  
 grinder@ua.fm 24

## Безопасность беспроводных сетей

Методы атак на беспроводные сети. Рекомендации по обеспечению безопасности.

**Виктор Игнатьев**  
 n4vy@nm.ru 28

## Сам себе антихакер. Защита от хакерских атак с помощью ipfw

Методы сбора доступной информации об объекте нападения и способы защиты от них с помощью пакетного фильтра ipfw.

**Сергей Супрунов**  
 amsand@rambler.ru 38

## Безопасность услуг хостинга

**Максим Костышин**  
 Maxim\_kostyshin@mail.ru 46

## АДМИНИСТРИРОВАНИЕ

## Rule Set Based Access Control для Linux

Обзор проекта RSABAC, решающего проблему разграничения доступа пользователей.

**Сергей Яремчук**  
 grinder@ua.fm 50

## Безумный чертенок

Знакомство с Frenzy – портативным инструментом системного администратора на базе ОС FreeBSD.

**Александр Байрак**  
 x01mer@pisem.net 58

## Эффективная работа с портами в FreeBSD

**Владимир Осинцев**  
 oc@nm.ru 62

## Почтовый сервер с защитой от спама и вирусов на основе FreeBSD

**Геннадий Дмитриев**  
 stranger03@mail.ru 68

## Безопасный удаленный доступ к консолям оборудования

**Дмитрий Ржавин**  
 d.rzhavin@rtcomm.ru  
**Рафаэль Шарафутдинов**  
 raphael@soft-tronik.ru 74

## ProxylInspector – инструмент контроля за расходованием интернет-трафика

**Андрей Бешков**  
 tigrisha@sysadmins.ru 80

## ПРОГРАММИРОВАНИЕ

## «Убиваем» зомби

Как писать программы без зомби.

**Андрей Уваров**  
 dashin@ua.fm 86

## ОБРАЗОВАНИЕ

## Active Directory – теория построения

**Иван Коробко**  
 ikorobko@prosv.ru 90