ОПЕРАЦИОННАЯ СИСТЕМА

(краткое описание)

ОГЛАВЛЕНИЕ

[1]КСЗИ – комплексная система защиты информации

Краткое вступление

В последнее время, словосочетание «*информационная безопасность*» можно встретить даже в областях достаточно далеких от мира ИТ[2]. Невероятно возросший информационный поток наложил на человечество свой отпечаток, но еще мало кто задумывается о том, что поток этот не только омывает все вокруг, но и вымывает из нас свои частицы, неся их на потеху первому встречному, который не поленится просто наклониться и подобрать это добро. Немногие из людей задумываются о том, какой информационный след оставляют они после себя. Ведь просто прийдя на работу или, скажем, поужинав в кафе - мы оставляем после себя частички информации о нас, о нашем образе жизни, о наших желаниях. И ЛЮБОЙ может узнать об этом, если ему это понадобится и если мы заранее не позаботимся о том, что же все-таки можно отдавать на откуп этому всепроникающему потоку.

Что уж говорить об областях человеческой деятельности где целостность информации – залог существования самой области. И где выбранное средство обеспечения безопасности определяет надежность всей системы в целом.

Одним из таких решений, позволяющих обеспечивать защиту информации и является проект BBOS.

Что такое BBOS

BBOS это операционная система общего назначения, основанная на базе свободной UNIX-подобной ОС[3] OpenBSD, жестко направленная на обеспечение целостности данных и безопасности функционирования.

Данная ОС может применяться как для решения задач сетевой инфраструктуры, так и задач, выполняемых пользовательской рабочей станцией.

Цели

Целью BBOS является обеспечение целостности данных, безопасности функционирования и разграничения доступа при работе с оберегаемой информацией, в условиях, когда используются публичные незащищенные информационные среды (например: Интернет).

Отличие BBOS от OpenBSD

Как было уже было сказано выше, родительской системой для BBOS является OpenBSD.

OpenBSD – это свободно распространяемая, многоплатформенная, UNIX-подобная операционная система, основанная на 4.4BSD, целями которой являются корректность, безопасность, стандартизация и портируемость. Кроме того, система делает изначальный упор на безопасность, что подтверждается ее большим сроком стабильного существования (за более чем 10-летний период всего две уязвимости в установке по умолчанию).

Неплохой старт для создания собственной ОС! Неправда ли?

Однако, несмотря на отличный функционал, предоставляемый OpenBSD, исходя из реальных потребностей ИТ отрасли, возникла необходимость в узкоспециализированной настройке и поведении ОС. В связи с этим, была проделана большая работа, которая впоследствии настолько изменила поведение первоначальной системы, что было принято решение об «отпочковании» проекта в самостоятельную операционную систему.

---

[2] Информационные технологии

[3] Операционная Система (ОС) – некая среда (одна суперпрограмма, или несколько программ), которая обеспечивает и контролирует выполнение постороннего программного кода изначально не предусмотренного, но работающего по ее правилам

Рассмотрим, чем же отличается функционал BBOS от стандартного функционала родительской OpenBSD.

Основные отличия:

- Аудит целостности критичных системных файлов (производится периодическая проверка целостности и, в завистимости от результатов проверки, система принимает решение о продолжении работы);
- Измененный вход в систему для непривилегированных пользователей. Кроме того создан дополнительный реестр легитимных пользователей (легитимное добавление/удаление пользователей осуществляется только средствами BBOS);
- Жесткое разграничение рабочего пространства непривилегированных пользователей (рабочее пространство активируется и становится доступным только по факту входа в систему);
- Отключение всех неиспользуемых для данной задачи процессов и множество дополнительных мелких настроек ОС, направленных на ужесточение безопасности, вплоть до ограничения некоторых возможностей суперпользователя[4].

Однако при всем этом, BBOS является OpenBSD-совместимой и все особенности OpenBSD будут справедливы и для BBOS.

Области применения

Как уже упоминалось выше, в качестве наследства OpenBSD, BBOS приобрела весь тот обширный задел программного обеспечения, который позволяет говорить о ней, как о системе общего назначения.

Кроме того, BBOS способна работать на многих архитектурах[5] таких, как:

- alpha
- amd64
- armish
- hp300
- hppa
- i386
- landisk
- mac68k
- macppc
- mvme68k
- mvme88k
- sgi
- socppc

[4] Аналог пользователя «`Администратор`» в Microsoft Windows – учетная запись, под которой разрешено **любое** действие в системе

[5] В компьютерной терминологии – может означать, как различный тип микропроцессоров, так и принципиально отличающийся подход к созданию вычислительных машин

- sparc
- sparc64
- vax
- zaurus

Это дает ей возможность найти применение в самом разнообразном качестве, начиная от узкоспециализированных серверных задач, заканчивая элементарным набором текстовой информации.

Рассмотрим задачи, для решения которых можно было бы применить BBOS:

- сервер баз данных

Для работы с базами данных BBOS предоставляет на выбор несколько программных продуктов:

- **MySQL 5.0.77** – свободная система управления базами данных (СУБД). MySQL является собственностью компании Sun Microsystems, осуществляющей разработку и поддержку приложения. Распространяется под GNU General Public License[6];
- **PostgreSQL 8.3.6** – свободная объектно-реляционная система управления базами данных (СУБД). Является свободной альтернативой коммерческим СУБД (таким как Oracle Database, Microsoft SQL Server, IBM DB2, Informix и СУБД производства Sybase) вместе с другими свободными СУБД (такими, как например, MySQL);

Все они являются свободными программными продуктами, со своими средами разработки, своими достоинствами и недостатками. Выбор той или иной СУБД определяется задачами, оборудованием, сложностью развертывания/освоения/перехода, наличием у обслуживающего персонала соответствующих знаний.

Здесь нужно заметить, что качеством, перечисленные выше программные продукты, не уступают своим коммерческим аналогам и вполне способны решать задачи такой же сложности и масштаба.

- почтовый сервер

Работа с почтой всегда была «коньком» UNIX-подобных систем. Здесь имеется множество программных продуктов для самых разнообразных задач, что позволяет использовать систему с максимальной эффективностью.

Необходимо заметить, что в мире UNIX понятие «электронная почта» разделено на несколько составляющих: есть программы которые занимаются только манипуляциями с корреспонденцией (отправка, доставка, отсеивание и проч.), есть программы предназначенные только для работы с уже полученными письмами и создания новых (доставка – это проблема других программ), есть продукты которые совмещают в себе и то и другое. Тут уж необходимо руководствоваться или имеющимся опытом, или рекомендациями специалистов, у которых этот опыт есть.

[6]GNU General Public License – лицензия на свободное программное обеспечение, созданная в рамках проекта GNU в 1988 г. Её также сокращённо называют GNU GPL или даже просто GPL, если из контекста понятно, что речь идёт именно о данной лицензии. Цель GNU GPL – предоставить пользователю права копировать, модифицировать и распространять (в том числе на коммерческой основе) программы, а также гарантировать, что и пользователи всех производных программ получат вышеперечисленные права.

Для почтового сервера можно использовать следующее программное обеспечение:

- **sendmail 8.14.3** – один из популярнейших агентов передачи почты (MTA – mail transfer agent). Распространяется бесплатно вместе с исходными кодами. Существуют версии программы для практически всех операционных систем и аппаратных платформ;

- **postfix 2.5.6** – агент передачи почты (MTA – mail transfer agent). Является свободным программным обеспечением. Postfix создавался как альтернатива Sendmail. Считается, что Postfix быстрее работает, легче в администрировании, более защищён и, что важно, совместим с Sendmail;

- **exim 4.69** - это полностью свободный агент передачи почты, используемый в операционных системах семейства Unix. Первая версия была написана в 1995 году Филиппом Гейзелом (Philip Hazel) для использования в качестве почтовой системы в Кембриджском Университете. У Exim прекрасная история безопасности и ни одной критической уязвимости с версии 4.xx. Распространяется под лицензией GPL;

Что касается программ для обработки почтовой корреспонденции (чтение писем, редактирование и проч.), то и здесь существует возможность выбора даже не столько между программными продуктами, сколько скорее между принципами работы этих программ.

Немного отступим от разговора о почте и поговорим вот о чем. BBOS, как и любая UNIX-подобная ОС позволяет осуществлять настройку и использование оборудования в удаленном режиме (т.н. терминальная сессия).

Что это значит?

Это значит, что компьютер (возьмем для примера самый обычный компьютер, который сейчас можно встретить и на работе и дома), который выполняет какую-то свою работу, под управлением BBOS может быть запущенным без монитора, мыши и клавиатуры. Администратор имеет возможность удаленно (из дома, с работы, вообще с любой точки мира) зайти на сервер, провести необходимую работу, и даже в таком режиме у него имеется возможность искать информацию в сети Интернет и использовать электронную почту. И для этого не нужно держать на сервере дорогое оборудование (например монитор), которое может быть использовано всего раз или два непосредственно.

Почтовые программы пользователя, которые могут быть использованы в режиме терминальной сессии:

- **mail** – простейший (и первый) почтовый клиент (MUA) для UNIX-подобных операционных систем, работающий в консольном режиме[7];

- **mutt 1.5.18** – почтовый клиент с текстовым интерфейсом для Unix-подобных операционных систем. Mutt поддерживает большинство форматов почтовых ящиков (в том числе mbox и Maildir) и протоколов (POP3, IMAP и т. д.). Также включает поддержку MIME, PGP/GPG и S/MIME-интеграцию. Распространяется по лицензии GPL;

- **alpine 2.00** – почтовый клиент для Unix-подобных систем с поддержкой UTF-8. Распространяется под весьма строгой лицензией. Пользователям доступны исходные тексты, но локальные модификации могут распространяться только в виде патчей и неофициальные версии должны быть четко отмечены, как таковые;

- **elm 2.4** – простой полноэкранный почтовый клиент для Unix-подобных систем;

[7]Во время терминальной сессии чаще всего доступен только алфавитно-цифрофой режим отображения информации. Т.е. – никакой графики. Такой режим и называется консольным.

Пользовательские почтовые программы с графическим интерфейсом:

- **KDE**[8] **kmail** – клиент электронной почты, созданный в рамках проекта KDE. Распространён в операционных системах семейства *nix. Поддерживает SMTP, POP3, IMAP, локальные почтовые ящики. Отображение писем в текстовом формате и в HTML с поддержкой различных кодировок. Есть возможности, повышающие удобства работы с письмами, включая цветовое выделение, фильтры, показ фотографий отправителя, привязанных к записям в адресной книге и т. д.;

- **evolution 2.24.4** – графическая клиентская программа управления электронной почтой, контактами и временем с открытым кодом, изначально написанная для платформы GNU/Linux. Создана фирмой Ximian, приобретённой в 2003 г. корпорацией Novell, которая с тех пор осуществляет разработку и поддержку продукта. С сентября 2004 года входит в состав оконной среды GNOME. Содержит календарь, систему планирования временем, адресную книгу. Поддерживает все распространённые почтовые протоколы – IMAP, POP, SMTP с аутентификацией через TLS. Evolution может соединяться с серверами Microsoft Exchange 2000/2003 и GroupWise. Кроме этого, программа поддерживает PGP/GnuPG для шифрования или электронной подписи сообщений, содержит Junk/Spam-фильтр;

- **sylpheed 2.5.0** – свободный легковесный почтовый и новостной клиент. Sylpheed предоставляет простоту конфигурации и, в то же время, изобилие функциональности. Поддержка не только основных почтовых протоколов вроде POP3, IMAP4rev1 и SMTP, но и NNTP (NetNews). Также по-умолчанию поддерживается и IPv6 – Интернет-протокол нового поколения;

- **mozilla-thunderbird 2.0** – бесплатная, кроссплатформенная, свободно распространяемая программа для работы с электронной почтой и группами новостей. Является составной частью проекта Mozilla. Поддерживает протоколы: SMTP, POP3, IMAP, NNTP, RSS.

Как видно, система имеет все возможности для решения задач, так или иначе связанных с электронной почтой.

- шлюз аутентификации и доступа

Если уж мы говорим о безопасности, то нам никак не обойтись без разговора о несанкционированном доступе.

BBOS имеет замечательный пакетный фильтр PF, доставшийся ей в наследство от OpenBSD. В сочетании с механизмом аутентификации authpf[9] это дает возможность регулировать доступ к ограничиваемой информации так гибко, как только это может понадобиться.

Контролировать можно все: кому входить в систему (вход в систему осуществляется при помощи SSH-клиента[10]), время входа, дисковые и процессорные руссурсы; даже место входа (можно разрешить доступ с конкретной и только этой машины в организации).

Кроме того, в системе постоянно ведется аудит действия пользователей, что при грамотном донесении до последних способно внести свой вклад в повышение безопасности.

И если такая ОС стоит на сервере, который обеспечивает взаимодействие с внешней средой (например: Интернет, чужая локальная сеть и проч.), то можно говорить о значительном снижении риска утечки оберегаемой информации.

---

[8] Популярный оконный менеджер.

[9] Работа с authpf - это тема для отдельного большого документа. Поэтому здесь будут упомянуты только основные принципы.

[10] Программа, предназначенная для удаленного входа в систему, позволяющая выполнять произвольные команды после успешного процесса аутентификации, который исключает возможность перехвата пересылаемой информации, т.к. вся информация шифруется перед отправкой.

Помимо этого BBOS имеет и свои средства проверки целостности и контроля доступа, так что в соовокупности системе есть что предоставить чужеродному воздействию, в случае, если такая ситуация возникнет[11].

- построение КСЗИ

Главной отличительной особенностью ОС BBOS является то, что она может быть использована[12] при построении комплексных систем защиты информации классов 2-3 (классификация согласно НД ТЗИ 2.5-005-99).

Согласно требований закона[13], вся информация, являющаяся собственностью государства, или информация с ограниченным доступом[14], должна обрабатываться в системе с применением комплексной системы защиты информации с подтвержденным соответствием. Подтверждение соответствия осуществляется по результатам государственной экспертизы в порядке, опередеденном законодательством.

Комплексные системы защиты информации (КСЗИ) представляют собой совокупность мероприятий, которые можно поделить на две основные категории:

- организационные;
- инженерно-технические.

Все эти мероприятия направлены на обеспечение защиты критичной информации от утечки, нарушения целостности и несанкционированного доступа.

Организационные мероприятия

Обеспечивают управление, документальное закрепление положений по информационной безопасности и определяют ответственность за нарушение установленного режима информационной безопасности.

Инженерно-технические мероприятия

Совокупность специальных технических средств[15] обеспечивающих установленный в организации режим безопасности и защиты информации. Выбор инженерно-технических мероприятий зависит от необходимого уровня защищенности информации.

Необходимость построения КСЗИ определяется требованием нормативных документов или желанием владельца информационных ресурсов.

- файловый и веб сервер

Если говорить о таких распространенных серверных задачах, как файл- или веб-сервер, то здесь BBOS может предложить следующие программные продукты:

---

[11]Известно, что нет абслоютно защищенных систем. Но поставить на пути злоумышленника щит, могущий отпугнуть последнего самой сложностью взлома – задача вполне осуществимая.

[12]Экспертное заключение № 158 от 04.12.2008. **Сертификацию прошла как сама ОС, так и весь комплект программного обеспечения для нее**.

[13]Постановление Кабинета Министров от 29.03.2006г. № 373

[14]Например: конфиденциальная информация.

[15]Согласно Закона Украины «О защите информации в информационно-телекоммуникационных системах» для создания комплексной системы защиты информации, являющейся собственностью государства, или информации с ограниченным доступом, требование к защите которой установлена законом, используются средства защиты информации, которые имеют сертификат соответствия или положительное экспертное заключение по результатам государственной экспертизы в сфере технической и/или криптографической защиты информации.

файл-сервер

- ftpd – простой FTP-сервер, идущий в поставке вместе с системой, тем не менее позволяющий организовать полноценный файл-сервер (например: для локальной сети большой организации).

- vsftpd 2.0.5 – FTP сервер являющийся безопасным, эффективным, стабильным, полностью готовым и проверенным решением в мире FTP серверов.

- pure-ftpd 1.0.21 – небольшой, легкий в настройке, быстрый и безопасный FTP сервер.

- sftp-server – неплохое решение, если нужно просто скопировать/передать несколько файлов. Входит в состав SSH-пакета. Все данные шифруются перед отправкой. На принимающей стороне должен быть использован клиент scp.

Кроме того, говоря о файл-серверах, нельзя не обойти стороной такое полезное решение, как *samba*.

Samba - программа, которая позволяет обращаться к сетевым дискам на различных операционных системах. Имеет клиентскую и серверную части. Является свободным программным обеспечением, выпущена под лицензией GNU. Также предоставляет службы файлов и печати для различных клиентов Microsoft Windows, и может интегрироваться с операционной системой Windows Server, либо как основной контроллер домена (PDC), либо как член домена.

Здесь необходимо отметить, что samba входит в комплект стандартного программного обеспечения, которое поставляется с ОС BBOS и может выполнять все функции Active Directory, не прибегая к услугам ОС Microsoft Windows.

веб-сервер

- apache 2.2.9 – свободный веб-сервер. Является самым популярным HTTP-сервером в Интернете. Основными достоинствами считаются надёжность и гибкость конфигурации. Он позволяет подключать внешние модули для предоставления данных, использовать СУБД для аутентификации пользователей, модифицировать сообщения об ошибках и т. д. Поддерживает IPv6.

- nginx 0.6.34 – свободный веб-сервер и почтовый прокси-сервер, работающий на Unix-подобных операционных системах.

- lighttpd 1.4.21 - веб-сервер, разрабатываемый с расчётом на быстроту и защищённость, а также соответствие стандартам. Это свободное программное обеспечение, распространяемое по лицензии BSD[16].

Как видно, система имеет все необходимые программные продукты для успешного решения подобных задач.

- терминальный сервер

Терминальный сервер – сервер, предоставляющий клиентам вычислительные ресурсы (процессорное время, память, дисковое пространство) для решения задач. Технически, терминальный сервер представляет собой очень мощный компьютер, соединенный по сети с терминальными

[16]Программная лицензия университета Беркли – это лицензионное соглашение, впервые применённое для распространения UNIX-подобных операционных систем BSD. Позже исходная версия лицензии была подвергнута ряду изменений, породив множество лицензий, обобщённо именуемых «лицензии типа BSD». В настоящее время лицензии типа BSD являются одними из самых популярных лицензий для свободного программного обеспечения и используются для многих программ.

клиентами которые, как правило, представляют собой маломощные или устаревшие рабочие станции или специализированные решения для доступа к терминальному серверу.

Терминальный клиент после установления связи с терминальным сервером пересылает на последний вводимые данные (нажатия клавиш, перемещения мыши) и, возможно, предоставляет доступ к локальным ресурсам (например, принтер, дисковые ресурсы, устройство чтения смарт-карт, локальные порты (COM/LPT)).

Терминальный сервер предоставляет среду для работы (терминальная сессия), в которой исполняются приложения пользователя. Результат работы сервера передается на клиент – как правило, это изображение для монитора и звук (при его наличии).

Преимущества терминального сервера

- Снижение временных расходов на администрирование.
- Повышение безопасности – снижение риска инсайдерских взломов.

Недостатки

- Концентрация всей функциональности в рамках одного (нескольких) серверов – выход из строя любого элемента между приложением и клиентами (сервер, коммутаторы, СКС) приводит к простою многих пользователей.
- Усиливаются негативные последствия ошибок конфигурации и работы ПО (последствия ошибок сказываются не на отдельных пользователях, а на всех пользователях сервера сразу же).

- тонкий клиент

Тонкий клиент в компьютерных технологиях – бездисковый компьютер-клиент в сетях с клиент-серверной или терминальной архитектурой, который переносит все или большую часть задач по обработке информации на сервер.

В настоящее время под термином «тонкий клиент» подразумевается достаточно широкий, с точки зрения системной архитектуры, ряд устройств, которые объединяются общим свойством: возможность работы в терминальном режиме. Таким образом, для работы тонкого клиента необходим терминальный сервер. Этим тонкий клиент отличается от толстого клиента, который, напротив, производит обработку информации независимо от сервера, используя последний в основном лишь для хранения данных. Примером тонкого клиента может служить компьютер с браузером, использующийся для работы с веб-приложениями.

Кроме общего случая, следует выделить аппаратный тонкий клиент – специализированное устройство, принципиально отличное от ПК. Аппаратный тонкий клиент не имеет жёсткого диска, использует специализированную локальную ОС (одна из задач которой организовать сессию с терминальным сервером для работы пользователя), не имеет в своём составе подвижных деталей, выполняется в специализированных корпусах с полностью пассивным охлаждением.

Для расширения функциональности тонкого клиента прибегают к его «утолщению», например, добавляют возможности автономной работы, сохраняя главное отличие – работу в сессии с терминальным сервером. Когда в клиенте появляются подвижные детали (жёсткие диски), появляются возможности автономной работы, он перестаёт быть тонким клиентом в чистом виде, а становится универсальным клиентом.

Тонкий клиент в большинстве случаев обладает минимальной аппаратной конфигурацией, вместо жёсткого диска для загрузки локальной специализированной ОС используется флеш-диск – в BIOS он определяется как обычный жёсткий диск, только размер его обычно значительно меньше.

В некоторых случаях тонкий клиент загружает операционную систему по сети с сервера, используя протоколы PXE, BOOTP, DHCP, TFTP и Remote Installation Services (RIS).

Подобная реализация тонкого клиента существует и с применением ОС BBOS.

В сравнении с Microsoft Windows

Как мы видим, ОС BBOS может охватить самый широкий спектр задач и возникает закономерный вопрос: «А можно ли заменить ею MS Windows», которая используется повсеместно.

Если сравнивать BBOS с Microsoft Windows, то здесь можно отметить одно неоспоримое преимущество – BBOS имеет абсолютный иммунитет к любому вирусу, поражающему компьютеры, работающие под управлением семейства Microsoft Windows. И если учесть настройки безопасности, которые предоставляет эта система, то в этом ключе она выглядит особо привлекательно.

Еще один немаловажный фактор – это то, что вместе с ОС BBOS поставляется огромный комплект программного обеспечения, за которое уже не нужно платить дополнительно (свыше 5000 пакетов: веб-браузеры, графические редакторы, текстовые редакторы, языки программирования и проч.) .

Конечно, кроме этого система имеет множество и других достоинств: повышенная стабильность (по сравнению с ОС Windows), гораздо бóльший уровень безопасности и разделения полномочий (если все настроено и работает – система может пребывать в таком состоянии неограниченно долгое время), для ее работы может применяться менее мощное (а значит и менее дорогое) оборудование, чем для ОС Windows, которая решает такие же или схожие задачи.

Однако существенным недостатком BBOS можно назвать ее повышенную сложность (как в освоении, так и в администрировании) по сравнению с операционными системами Microsoft Windows.

Поэтому, сначала категорически необходим анализ построения компьютерной инфраструктуры с тем, чтобы верно определить задачи, которые она должна обеспечивать. Вероятно, что ОС BBOS сможет обеспечить значительный процент тех задач, для которых в данный момент применяется ОС Microsoft Windows и с не меньшим качеством (например: рабочее место секретаря или менеджера).

Для наглядности приведем сравнительную таблицу критических моментов, могущих повлиять на выбор ОС:

	Подверженность вирусам	Дополнительное ПО	Устойчивость к атакам	Простота освоения
BBOS	· · ·	★★★★★	★★★★★	★★
MS Windows	★★★★★	★	★★	★★★★★

Итоги

Если кратко подытожить, то можно утверждать, что система способна выполнять большинство задач (здесь не учитываются узкоспециализированные задачи), которые в данный момент повсеместно выполняются на ОС Windows.

Поэтому можно предположить, что часто востребуемым функционалом ОС BBOS будут следующие реализации:

- сервера баз данных;
- почтового сервера;

- шлюза аутентификации и доступа;
- криптографического элемента некоей сложной информационной системы (например: шифрование передаваемой информации);
- файлового сервера;
- веб сервера;
- отказоустойчивого сетевого экрана;
- детектора и защиты от атак (в частности DDOS-атак);
- прослойки для обеспечния работы тонкого клиента, и одновременно его среды;
- прочее.