

## БЕЗОПАСНОСТЬ В IBM System Z – ВЫСОЧАЙШИЙ СТАНДАРТ КАЧЕСТВА СЕГОДНЯ, ГОТОВНОСТЬ К ИЗМЕНЯЮЩИМСЯ И РАСТУЩИМ ТРЕБОВАНИЯМ РЫНКА ЗАВТРА

### Мэйнфреймы IBM как ядро системы управления информационной безопасностью предприятия

На протяжении всей более чем 40-летней истории развития платформы мэйнфреймов (ныне IBM System Z) компания IBM целенаправленно придерживалась концепции как можно более тесной интеграции аппаратных средств и программного обеспечения. В результате серверы IBM System Z сегодня представляют собой системы с богатым набором средств обеспечения безопасности на нескольких уровнях: аппаратном, операционной системы, СУБД, а также на уровне специализированного программного обеспечения, как прикладного, так и промежуточного (middleware).

Серверы IBM System z9™ бизнес-класса (BC) и масштаба предприятия (EC) в комплексе с программным обеспечением предоставляют высочайший уровень информационной безопасности и возможность блокировки практически любых нарушений политики безопасности на предприятии. Сюда входят: защита данных, используемых совместно с доверенными партнерами, реализуемая с помощью совершенных криптографических средств, защита персональной информации пользователя, а также данных, передаваемых по сети. При этом обеспечивается высочайший уровень доступности серверов, приложений и, что самое главное – данных.

### Бизнес-среда, насыщенная средствами безопасности



### Средства безопасности, встроенные в оборудование System Z:

#### Аппаратная поддержка (CPACF) для выполнения криптографической функции

- Обеспечивает симметричное шифрование с использованием незашифрованного ключа
- Входит в состав центральных процессоров всех систем IBM System z9 EC и BC, серверов IBM eServer™ zSeries® 990 и 890 (z990, z890), включая специализированные процессоры для Linux (Integrated Facility for Linux® – IFL)
- Серверы z9 EC и z9 BC поддерживают расширенный стандарт шифрования (AES) с ключами длиной 128 бит, хэш-функцию SHA-256 и генератор псевдослучайных чисел (PRNG)
- Дополнительная информация приведена по следующему интернет-адресу:  
[ibm.com/servers/eserver/zseries/security/features.html](http://ibm.com/servers/eserver/zseries/security/features.html)

#### Дополнительная аппаратная возможность – Crypto Express2

- Обеспечивает шифрование с использованием зашифрованного ключа
- Предлагается для систем z9 EC, z9 BC, z990 и z890
- Может быть гибко сконфигурирована как криптографический сопроцессор или акселератор
- Дополнительная информация приведена по следующему интернет-адресу:  
[ibm.com/servers/eserver/zseries/security/features.html](http://ibm.com/servers/eserver/zseries/security/features.html)

## **LPAR-PR/SM™ – механизм разбиения сервера на логические разделы**

Приложения в разных логических разделах абсолютно изолированы друг от друга. Имеется сертификация уровня EAL5 по единым критериям.

- Поддерживает большое количество прикладных программ, использующих данные и работающих в среде операционных систем z/OS®, z/VM® и Linux
- Архитектура системы предотвращает саму возможность каких-либо информационных потоков между логическими разделами, помимо штатного протокола обмена (механизм обмена память – память, т.н. HyperSocket™)
- Дополнительная информация приведена по следующему интернет-адресу: [ibm.com/servers/eserver/zseries/security/features.html](http://ibm.com/servers/eserver/zseries/security/features.html)

## **Средства безопасности z/OS:**

В состав операционной системы z/OS входят следующие средства защиты информации:

### **ICSF – Интегрированная служба криптографии**

- Обеспечивает возможности централизованного управления ключами и аутентификации доступа
- Поддерживает в z/OS сервисы инфраструктуры открытых ключей (PKI) и средства шифрования
- Дополнительная информация приведена по следующему интернет-адресу: [ibm.com/systems/systemz9/feature092705/](http://ibm.com/systems/systemz9/feature092705/)

### **PKI – служба инфраструктуры открытых ключей**

- Может использоваться в качестве удостоверяющего центра (Certificate Authority – CA), выпускающего цифровые сертификаты
- Осуществляет управление жизненным циклом цифровых сертификатов
- Имеет сертификацию Identrus (см. информацию на интернет-странице: [ibm.com/servers/eserver/zseries/security/identrus/](http://ibm.com/servers/eserver/zseries/security/identrus/))
- Дополнительная информация приведена по следующему интернет-адресу: [ibm.com/servers/eserver/zseries/zos/pki/](http://ibm.com/servers/eserver/zseries/zos/pki/)



### **MLS – многоуровневая защита**

- Обеспечивает разграничение доступа на уровне строк таблиц в СУБД DB2®
- Позволяет создавать единые базы данных, оснащенные средствами защиты информации
- Обеспечивает соблюдение требований безопасности при доступе к данным со стороны нескольких различных групп пользователей одновременно
- Дополнительная информация приведена по следующему интернет-адресу: [ibm.com/servers/eserver/zseries/security/mls.html](http://ibm.com/servers/eserver/zseries/security/mls.html)

## **Сетевая безопасность сервера коммуникаций z/OS:**

**IPSec и Application Transparent TLS** – открытые протоколы сетевой безопасности, предлагающие стойкую криптозащиту данных, передаваемых по сети

- Разработаны, чтобы свести к минимуму необходимость изменения исходного кода прикладных программ и ускорить их развертывание
- Конфигурирование на основе политик – упрощение контроля соответствия требованиям безопасности
- Для ускорения криптографических операций используются аппаратные средства безопасности System Z (см. выше)
- Программа настройки конфигурации защиты сети (NSCA) помогает упростить администрирование
- Дополнительная информация приведена по следующему интернет-адресу: [ibm.com/software/network/commsserver/zos/security/](http://ibm.com/software/network/commsserver/zos/security/)

**IDS** – служба обнаружения вторжений, защищающая System Z от атак со стороны сети.

- Разработана, чтобы обнаруживать в реальном времени как известные, так и новые виды атак
- Активизирует защитные механизмы на сервере z/OS.
- Дополнительная информация приведена по следующему интернет-адресу: [ibm.com/servers/eserver/zseries/zos/commsserver/intrusion\\_detection.html](http://ibm.com/servers/eserver/zseries/zos/commsserver/intrusion_detection.html)

### Широкий выбор прикладных программ системы безопасности:

RACF® – предлагает централизованные функции защиты, такие как идентификация и проверка подлинности пользователей, управление доступом к ресурсам системы и ее аудит. Контролирует действия как самой операционной системы, так и выполняемых в ее среде прикладных программ.

- Дополнительная информация приведена по следующему интернет-адресу:  
[ibm.com/servers/eserver/zseries/zos/racf/](http://ibm.com/servers/eserver/zseries/zos/racf/)

**\*Новое!\*** **Encryption Facility for z/OS** – устанавливаемое на сервере программное решение, обеспечивающее защиту данных от утраты или порчи в результате неосторожных или умышленных действий.

- Обеспечивает долгосрочное управление ключами шифрования архивных данных и информации, предназначенной для обмена с удаленными подразделениями и партнерами
- Позволяет серверам z/OS обмениваться зашифрованными данными с серверами, работающими под управлением других операционных систем
- Дополнительная информация приведена по следующему интернет-адресу:  
[ibm.com/servers/eserver/zseries/zos/encryption\\_facility/](http://ibm.com/servers/eserver/zseries/zos/encryption_facility/)

### Tivoli:

#### Tivoli® Access Manager for e-business

#### Tivoli Access Manager for Business Integration Host Edition (TAMBI-HE)

Обеспечивают безопасность для бизнеса по требованию, включая однократный логический вход в систему через Интернет, удаленное администрирование через Интернет, а также защиту на основе политик.

**Tivoli Directory Integrator** предоставляет основанное на открытой архитектуре метакаталога решение для синхронизации и обмена информацией в реальном времени между прикладными программами или такими источниками данных, как оглавления.

**Tivoli Directory Server** предлагает мощную инфраструктуру пользовательских учетных данных (Identity), построенную с использованием протокола LDAP, которая является фундаментом для развертывания комплексных систем контроля подлинности и управления учетными данными, а также иных передовых архитектур программного обеспечения.

- Дополнительная информация о Tivoli приведена на интернет-странице [ibm.com/software/Tivoli/Solutions/security](http://ibm.com/software/Tivoli/Solutions/security)

### Прикладные программы безопасности Vanguard:

- Защита систем с помощью Vanguard Explorer
- Управление пользователями с помощью Vanguard SecurityCenter и Vanguard Administrator
- Управление угрозами с помощью Vanguard Analyzer
- Достижение целей контроля соответствия требованиям безопасности с помощью Vanguard Explorer и Vanguard Advisor
- Дополнительная информация приведена на интернет-странице [ibm.com/software/tivoli/features/ccr2/ccr2-2005-08/feature-sysplex.html](http://ibm.com/software/tivoli/features/ccr2/ccr2-2005-08/feature-sysplex.html)

### Сертификация безопасности по общим критериям:

- Криптография IBM имеет самый высокий в отрасли рейтинг оборудования – FIPS 140-2 уровень 4
- Разбиение на логические разделы (LPAR-PR/SM), предлагаемое в системах z9 EC, z9 BC, z990 и z890, имеет сертификацию EAL5
- z/OS 1.7 с дополнительной возможностью RACF – имеет сертификацию EAL4+ по профилям CAPP (Профиль управляемого доступа – Controlled access protection profile) и LSPP (Профиль меток доступа – Labeled security protection profile)
- SUSE Linux Enterprise Server 9 имеет сертификацию безопасности EAL4+ по профилю CAPP
- z/VM V5.1 имеет сертификацию безопасности EAL3+ по профилям CAPP и LSPP
- Дополнительная информация приведена по следующему интернет-адресу:  
[ibm.com/security/standards/st\\_evaluations.shtml](http://ibm.com/security/standards/st_evaluations.shtml)





#### **IBM Восточная Европа/Азия**

Главная страница Web-сайта IBM находится по адресу **ibm.com**

IBM, логотип IBM, AIX, AIX 5L, eServer, System z, Tivoli, Virtualization Engine, xSeries являются товарными знаками International Business Machines Corporation в США и/или других странах.

Другие названия компаний, продуктов и услуг могут являться товарными знаками или знаками обслуживания соответствующих компаний.

Упоминание в этой публикации продуктов или услуг корпорации IBM не означает, что IBM предполагает предоставлять их во всех странах, где она ведет свою деятельность. Любые ссылки на продукты, программы и услуги корпорации IBM не означают, что можно использовать только продукты, программы и услуги корпорации IBM. Вместо них можно использовать любые аналогичные по своей функциональности продукты, программы и услуги.

Эта статья является иллюстрацией того, как один из клиентов IBM использовал технологии и/или услуги IBM и/или ее бизнес-партнеров. Описанные результаты и преимущества зависят от многих факторов. IBM не гарантирует получение сравнимых результатов. Вся информация в настоящем документе предоставлена клиентом и/или бизнес-партнером, и корпорация IBM не гарантирует ее точности.

Аппаратные продукты IBM производятся из новых компонентов или из новых и бывших в употреблении компонентов. Это обстоятельство не влияет на условия гарантии.

Данная публикация предназначена только для общего руководства.

На фотографиях могут быть показаны опытные образцы продукции.

© Copyright IBM Corporation 2007.

Все права защищены.