



ЛИНС-М

Информационная безопасность для
компаний финансового сектора

Практический опыт построения системы централизованного мониторинга ИБ в банковской организации на базе решений Oracle

13 февраля 2008г.

Волков Константин
Технический директор
Компания ЛИНС-М
kvolkov1@lins-m.ru

Содержание:

- О компании ЛИНС-М
- Задачи мониторинга ИБ, архитектура решения
- Источники данных системы
- Роли системы
- Интерфейс пользователя системы
- Результаты внедрения системы
- Соответствие требованиям стандартов

О компании ЛИНС-М

Партнеры:

ORACLE®



EMC²
where information lives™



netForensics®

SYSGEM®



McAfee®

Клиенты:

- Центральный Банк Российской Федерации
- Банк ВТБ
- Внешэкономбанк
- Транстелеком
- Cisco Systems
- и другие

О компании ЛИНС-М



ЛИНС-М:

- Соучредитель сообщества ABISS: Association for Banking Information Security Standards
- Разработчик Стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0



Мониторинг ИБ: СТО БР ИББС-1.0

П.10.9 СТО БР ИББС-1.0:

- Основными целями мониторинга ИБ в организации являются оперативное и постоянное наблюдение, сбор, анализ и обработка данных под заданные руководством цели. Такими целями анализа могут быть:
 - контроль за реализацией положений нормативных актов по обеспечению ИБ в организации;
 - выявление нештатных (или злоумышленных) действий в АБС организации;
 - выявление инцидентов ИБ.
- Для целей оперативного и постоянного наблюдения объектов мониторинга могут использоваться как специализированные (например, программные) средства, так и штатные (входящие в коммерческие продукты и системы) средства регистрации действий пользователей, процессов и т.п.



Мониторинг ИБ

- Процесс мониторинга ИБ является неотъемлемой частью деятельности по управлению ИБ
- Мониторинг ИБ – информационная основа для принятия решений
- Мониторинг ИБ - свидетельство оценок состояния ИБ организации



Мониторинг ИБ

Проблемы при мониторинге ИБ:



Решение

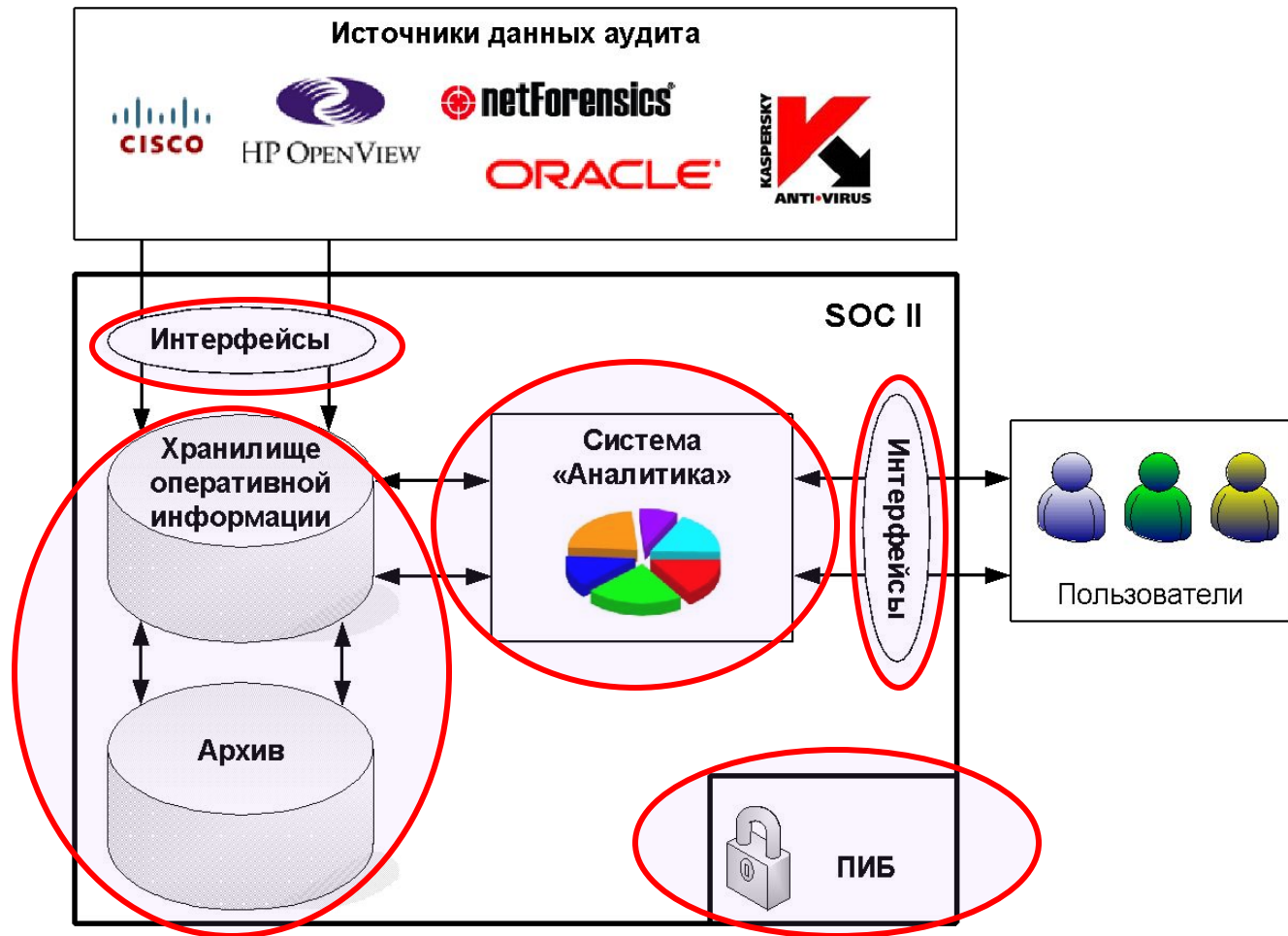
Центр координации деятельности по ИБ Security Operations Center Information Intelligence (SOC II)

SOC II предназначен:

- для анализа соответствия текущего уровня информационной безопасности принятым в организации требованиям
- для обеспечения целостности, защиты от подмены и уничтожения данных аудита ИБ ресурсов организации
- для обеспечения централизованной обработки данных аудита ИБ, агрегируемых при сборе от существующих систем мониторинга ИБ
- для генерации отчетности различных уровней детализации по результатам анализа данных аудита ИБ



Архитектура решения SOC II



Архитектура решения SOC II

Интерфейсы:

- Oracle Warehouse Builder
- Средства репликации СУБД Oracle.

Хранение данных и архивирование:

- СУБД Oracle 10g Enterprise Edition
- Oracle ILM Assistant

Аналитика и предоставление отчетности:

- Собственные разработки ЛИНС-М
- Oracle Business Intelligence Suite

Подсистема информационной безопасности:

- Oracle Database Vault

Источники данных SOC II

Источники данных SOC II

Существующие в организации системы мониторинга и СЗИ

Например: ПАК Аккорд, семейство HP OpenView, семейство IBM Tivoli, семейство CiscoWorks, средства мониторинга и управления операционными системами, сервера RADIUS, TACACS+ и т.д.

Активное сетевое оборудование, ОС



Security Operations Center (SOC)



Источники данных SOC II

Поддерживаемые форматы данных аудита ИБ:

- базы данных
- таблицы баз данных
- структурированные ascii файлы
- записи syslog
- *любые форматы*, поддерживаемые Oracle Warehouse Builder



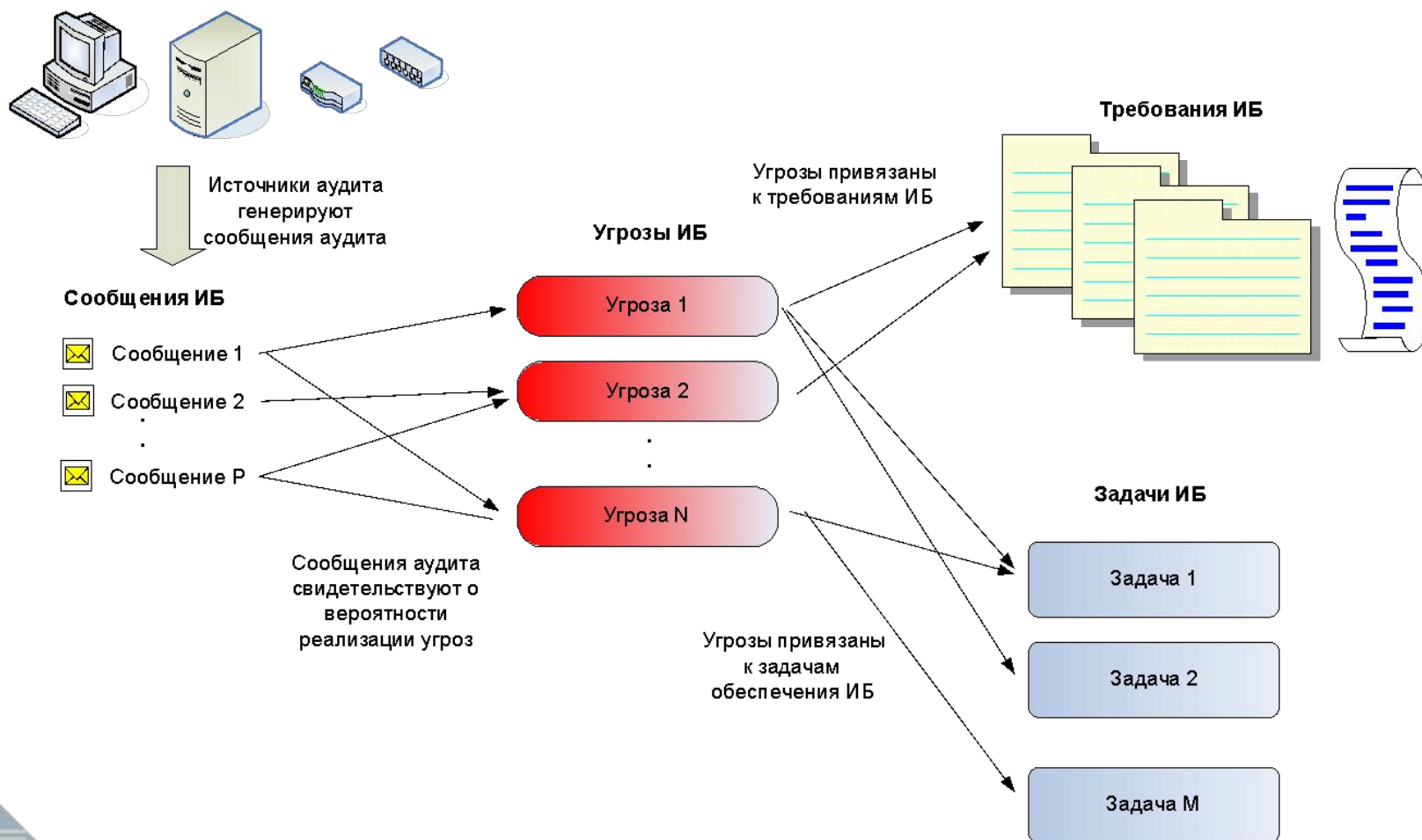
Роли системы

SOC II предполагает наличие в структуре Банка следующих ролей:

- **[Оператор]**: отслеживание событий, информирование Офицера ИБ об отклонениях
- **[Аналитик]**: расследование инцидентов ИБ, анализ изменений и трендов
- **[Офицер ИБ]**: общее управление, отвечает за ИБ
- **[Администратор БД SOC II]**: обслуживание БД
- **[Специалист по настройке]**: внесение изменений в настройки SOC II



Логика работы системы



Интерфейс

SOC II

My Dashboard Welcome, Administrator! Alerts! - Dashboards - Answers - More Products - Settings - Log Out

Главная страница | Задачи обеспечения ИБ | Угрозы | Нормативная документация по ИБ | Оборудование | Рекомендации | Динамика событий | Проверка доступности | Все сообщения | Page Options

Alerts!

Система мониторинга зафиксировала ошибки

Нарушения в задачах

Задачи обеспечения ИБ	Состояние
Защита от вирусной активности в банковской сети	🔴
Изоляция сегмента разработки	🔴
Контроль изменений физической/логической структуры сети	🔴
Мониторинг средств защиты сетей филиалов	🔴
Обеспечение работоспособности периметра ЛВС Банка	🔴

Сообщений за день

Уровни инфраструктуры

Time run: 08.02.08 10:18:03

Уровень	Оперативность	Состояние
1 Физический	☆☆☆☆	🟢
2 Сетевой	☆☆☆☆	🔴
3 Сетевых сервисов	☆☆☆☆	🟢
4 Операционных систем	☆☆☆☆	🟢
5 Систем управления БД	☆☆☆☆	🟢
6 Прикладного ПО	☆☆☆☆	🟢

30 Последних сообщений

17.02.08 17:01:43 в логах СЦМ %FW-6-SESS_AUDIT_TRAIL: tcp session initiator (172.30.0.111:4241) sent 777 bytes -- responder (209.85.66.224:80) sent 1112 bytes

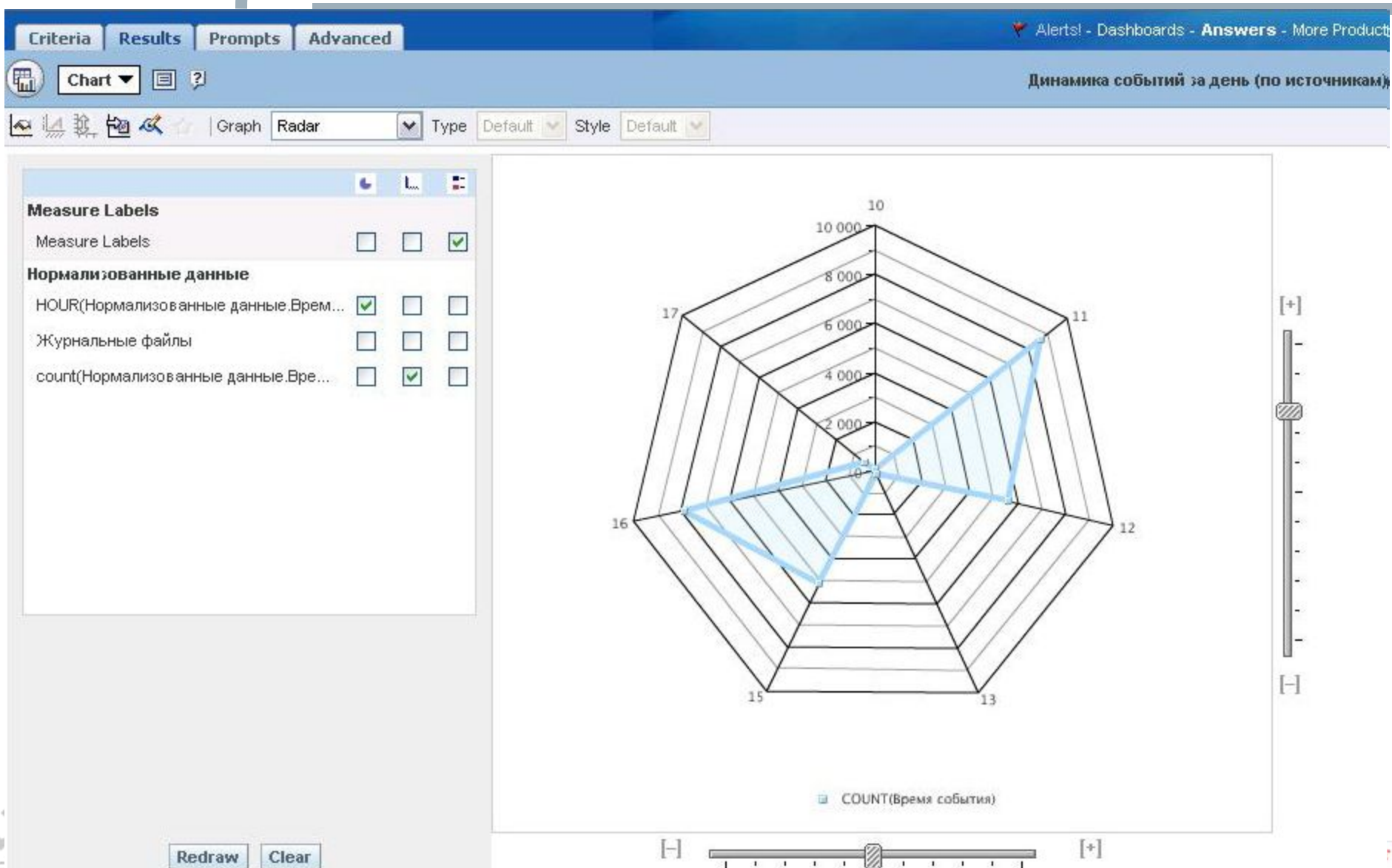
17.02.08 17:01:43 в логах СЦМ %FW-6-SESS_AUDIT_TRAIL: tcp session initiator (172.30.0.111:4242) sent 696 bytes -- responder (217.199.217.5:80) sent 96247 bytes

17.02.08 17:01:43 в логах СЦМ %FW-6-SESS_AUDIT_TRAIL: tcp session initiator (172.30.0.111:4243) sent 709 bytes -- responder (81.176.228.22:80) sent 0 bytes

17.02.08 17:04:42 в логах СЦМ %FW-6-SESS_AUDIT_TRAIL: tcp session initiator (172.30.0.111:4244) sent 712 bytes -- responder (81.176.228.22:80) sent 0 bytes




Интерфейс





Интерфейс: угрозы

Угрозы: представление информации по оборудованию

 **Виды оборудования и ОС**
предоставление информации о состоянии ИБ инфраструктуры

Вид оборудования

Оборудование	IP	Угрозы	Уровень	Оперативность	Состояние
CISCO--NF	172.030.000.104	Выполнение ошибочных или несанкционированных действий на сервере	Систем управления БД		
LINS-SERVER	172.030.000.106	Некорректная работа электронной почты	Прикладного ПО		
		Несанкционированный доступ к ресурсам по протоколам прикладного уровня	Сетевых сервисов		
ORACLE-EHD	172.030.000.019	Выполнение ошибочных или несанкционированных действий с БД	Систем управления БД		

powered by ORACLE



Интерфейс: угрозы

Угрозы: представление информации по территориальному признаку

Оборудование	IP	Угрозы	Уровень	Оперативность	Состояние
Иркутск	[REDACTED]	Нарушения правил маршрутизации и передачи данных	Сетевой	☆☆☆☆☆	🟢
		Сбои программно-аппаратной платформы локального маршрутизатора (ios)	Сетевой	☆☆☆☆☆	🟡
		Некорректная работа STP	Сетевой	☆☆☆☆☆	🟢
		Некорректная работа сервисов	Сетевых сервисов	☆☆☆☆☆	🟢
		Некорректная работа сервисов передачи мультимедийной информации	Сетевых сервисов	☆☆☆☆☆	🟢
		Несанкционированное или ошибочное изменение в локальной базе пользователей	Сетевой	☆☆☆☆☆	🟢
		<u>Несанкционированное или ошибочное изменение конфигурационных файлов</u>	Сетевой	☆☆☆☆☆	🔴
		Превышение ограничений на количество соединений и размер пакетов	Сетевой	☆☆☆☆☆	🟢
Курск	[REDACTED]	Нарушения правил маршрутизации и передачи данных	Сетевой	☆☆☆☆☆	🟢
		Несанкционированный сетевой доступ	Сетевых сервисов	☆☆☆☆☆	🟢
		Сбои программно-аппаратной платформы локального маршрутизатора (ios)	Сетевой	☆☆☆☆☆	🟡
		Некорректная работа STP	Сетевой	☆☆☆☆☆	🟢
		Некорректная работа сервисов	Сетевых сервисов	☆☆☆☆☆	🟢
		Некорректная работа сервисов передачи мультимедийной информации	Сетевых сервисов	☆☆☆☆☆	🟢
		Несанкционированное или ошибочное изменение в локальной базе пользователей	Сетевой	☆☆☆☆☆	🟢
		Несанкционированное или ошибочное изменение конфигурационных файлов	Сетевой	☆☆☆☆☆	🔴
		Превышение ограничений на количество соединений и размер пакетов	Сетевой	☆☆☆☆☆	🟢
Сбои программно-аппаратной платформы локального маршрутизатора (ios)	Сетевой	☆☆☆☆☆	🟡		

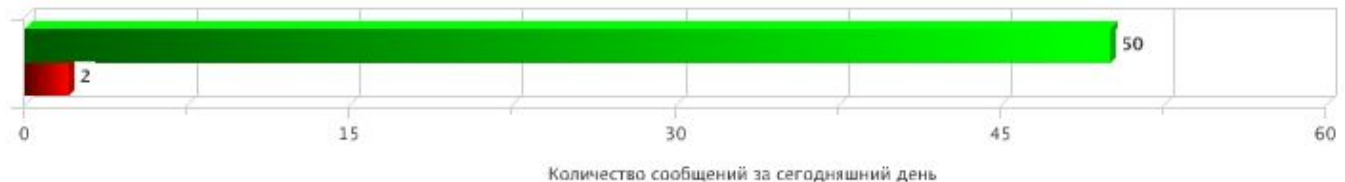
Интерфейс: детализация



Индикатор угрозы

Угроза

Несанкционированное или ошибочное изменение конфигурационных файлов



[Возврат \(Return\)](#)

Время события	Текст сообщения	Источник	Состояние
06.02.08 13:33:38	"Device\VMnet\User1" VNet version is incorrect, reinstall drivers	СКЛ-Windows	
06.02.08 13:22:04	"Device\VMnet\User1" VNet version is incorrect, reinstall drivers	СКЛ-Windows	

Щелкните

Время события	Текст сообщения	Источник	Состояние
06.02.08 13:33:38	"Device\VMnet\User1" VNet version is incorrect, reinstall drivers	СКЛ-Windows	
06.02.08 13:22:04	"Device\VMnet\User1" VNet version is incorrect, reinstall drivers	СКЛ-Windows	



Интерфейс: задачи ИБ

Подсистема
отображения
данных

Добро пожаловать,
Administrator!

Сигналы!

Информационные
панели

Ответы

Другие
программы

Настройка

Завершение
сеанса

Главная
страница

Задачи
обеспечения
ИБ

Угрозы

Нормативная
документация
по ИБ

Оборудование

Рекомендации

Динамика
событий

Проверка
доступности

Все
сообщения

Параметры

Задачи обеспечения ИБ

Время запуска: 08.02.08 13:18:55

Задачи обеспечения ИБ	Состояние
Защита от вирусной активности в банковской сети	
Защита от вирусных штормов в периметре	
Изоляция сегмента разработки	
Контроль изменений физической/логической структуры сети	
Мониторинг средств защиты сетей филиалов	
Обеспечение работоспособности периметра ЛВС Банка	



powered by ORACLE



Интерфейс: требования ИБ

My Dashboard

Welcome, Administrator! [Dashboards](#) - [Answers](#) - [More Products](#) - [Settings](#) - [Log Out](#)

Состояние ИБ

Приложение 1

Приложение 2

IP-активность

Нормативные документы

Все сообщения

Page Options



Нормативные документы

Предоставление информации о выполнении требований нормативных документов

Документ	Раздел документа	Группа параметров	TEXT	Критичность
СТО БР ИББС-1.0-2006	8.2.4. Общие требования по обеспечению информационной безопасности при управлении доступом и регистрации	Аутентификация и авторизация	%PIX-2-109011: Authen Session Start: user, sid number	Critical
			%PIX-3-109013: User must authenticate before using this service	Critical
			%PIX-3-109018: Downloaded ACL acl_ID is empty	Major
			%PIX-3-302302: ACL = deny; no sa created	Major
			%PIX-4-409023: Attempting AAA Fallback method <method_name> for <request_type> request for user <username> :Auth-server group <server_tag> unreachable	Minor
			%PIX-5-611103: User logged out: Uname: user	Warning
		Изменение в локальной базе пользователей	%PIX-6-109024: Authorization denied from source_IP_Address/src_port to dest_IP_Address/dest_port (not authenticated) on interface interface_name using protocol	Informational
			%PIX-6-109025: Authorization denied (acl=acl_ID) for user fromsource_address/source_port to dest_address/dest_port on interface interface_name using protocol	Informational
			%PIX-5-111003: IP_address Erase configuration	Informational
			%PIX-5-111005: IP_address end configuration: OK	Informational

powered by ORACLE

Интерфейс: требования ИБ

ISO/IEC 27001:2005	A.10.06.1 Средства контроля сетевых ресурсов	Некорректная работа сервисов передачи мультимедийной информации		
		Несанкционированное или ошибочное изменение конфигурационных файлов		
		Несанкционированный доступ к ресурсам по протоколам прикладного уровня		
		Ошибки ПО на АРМе		
		Сбои программно-аппаратной платформы локального маршрутизатора (ios)		
		Сбои программно-аппаратной платформы локального межсетевое экрана (PIX)		
		Сбой защищенного соединения		
	A.10.08.4 Электронный обмен сообщениями	Некорректная работа электронной почты		
	A.10.10 Мониторинг	Выполнение ошибочных или несанкционированных действий с БД		
		Сбои или некорректное восстановление работы подсистем вычислительной сети		

Оповещения и отчетность

Механизмы отчетности:

- Генерация отчетности в формате pdf/doc/html **на основании шаблонов, принятых в организации**
- Автоматическая e-mail рассылка отчетов заданным адресатам
- Генерация отчетности по расписанию

Механизмы оповещений:

- E-mail
- IM-сообщения
- Звуковые уведомления



Результаты внедрения

До внедрения SOC II

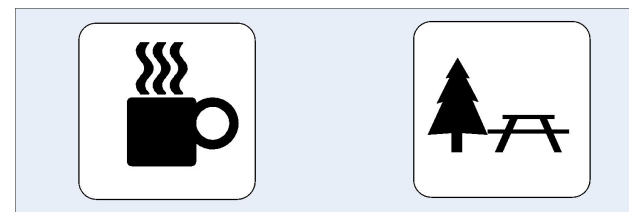
Соответствие требованиям ИБ ?
Эффективное выполнение задач ИБ ?
Целостная картина ?
Должен разбираться во всех технических средствах ?
Как обеспечить целостность и неизменность ?
Что делать ?

Ответственный за ИБ

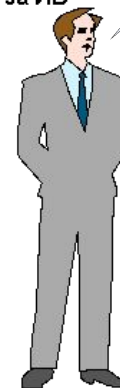


После внедрения SOC II

- ✓ Регулярная отчетность о выполнении требований ИБ
- ✓ Оперативный мониторинг задач обеспечения ИБ
- ✓ Общая картина по ИБ организации
- ✓ Не нужно вникать в технические детали по каждому источнику
- ✓ Данные аудита ИБ хранятся в защищенном хранилище, обеспечивающем их целостность и неизменность



Ответственный за ИБ



Соответствие стандартам

Соответствие требованиям СТО БР ИББС-1.0:

- п. 5.13 – процессный подход, включающий мониторинг
- п. 9.2 - реализация процесса обнаружения и реагирования на инциденты безопасности
- п. 9.3 - мониторинг и контроль защитных мер
- п.9.7 – полномочия и действия службы информационной безопасности
- п. 10.5 – журналы регистрации инцидентов ИБ
- п.10.9 - обнаружение и регистрации отклонений функционирования защитных мер от требований ИБ



Соответствие стандартам

Соответствие требованиям ISO 27001:2005

- Раздел А.10.10 Мониторинг:
 - Ведение журналов аудита
 - Мониторинг использования систем
 - Защита информации журналов регистрации
 - Журналы регистрации администратора и оператора
 - Регистрация неисправностей
- Раздел А.10.13 Менеджмент инцидентов ИБ:
 - Сообщение о событиях информационной безопасности
 - Изучение инцидентов информационной безопасности
 - Сбор свидетельств

И т.д.



ЛИНС-М

**Спасибо за
внимание!**

Волков Константин
Технический директор
kvolkov@lins-m.ru

