ГАЗПРОМБАНК

«Газпромбанк»
(Открытое акционерное общество)

Опыт создания Центра управления инцидентами информационной безопасности (Security Operation Center – SOC) в крупном Российском Банке.

Февраль 2013

ГАЗПРОМБАНК

Предпосылки проекта

1. Большое количество оборудования

- Более 6000 АРМ.
- Более 1500 серверов.
- Более 600 объектов активного оборудования.
- Более 500 автоматизированных систем и приложений.

2. Сложность ИТ - ландшафта

- Разнообразные ОС (ОС Novell, ОС Windows Server, ОС Red Hat Enterprise Linux, ОС SUSE Linux Enterprise Server, ОС HP-UX , ОС Solaris , ОС AIX , ОС OS/400 , ОС QNX , ОС SecurePlatform)
- Разнообразные СУБД (Oracle, Sybase, Microsoft SQL , Pervasive SQL , DB2, MySQL, Paradox, Interbase)

3. Различный возраст программных и технических средств (создание Банка в июле 1990 г.)

ГАЗПРОМБАНК

Предпосылки проекта

4. Большое количество «не контролируемых» инцидентов

по ДОСТУПНОСТИ:

- сбои в работе серверов;
- сбои в работе активного сетевого оборудования
- нарушение работоспособности автоматизированных систем и приложений

по КОНФИДЕНЦИАЛЬНОСТИ:

- несанкционированный доступ к информационно-техническим средствам
- неконтролируемая работа с внешними устройствами

по ЦЕЛОСТНОСТИ:

- несанкционированная модификация БД
- внесение несанкционированных изменений в транзакции
- внесение несанкционированных изменений в описание клиента

Концепция создания SOC

Объекты мониторинга

- Сервера, рабочие станции
- Активное сетевое оборудование
- Сетевые сервисы
- Операционные системы
- СУБД
- Автоматизированные системы и приложения
- СЗИ

Средства мониторинга

NagVis

Ready for IBM Tivoli software

IPSWITCH WhatsUpGold

ArcSight

Средство сбора и агрегирования

ArcSight

ArcSight

события с признаками инцидента

Система визуализации

Система расследования

(содержание, место, объект ИБ, ущерб и т.д.)

ca technologies

ИНЦИДЕНТЫ

Локализация, противодействие, минимизация ущерба

ГАЗПРОМБАНК

Технология работы

Основные этапы процесса выявление инцидентов ИБ:

- сбор информации;
- выявление корреляционных связей;
- формирование новых правил корреляции
- расследование инцидентов;
- проведение мероприятий, связанных с устранением последствий инцидентов или условий, вызвавших инцидент

ГАЗПРОМБАНК

Технология работы

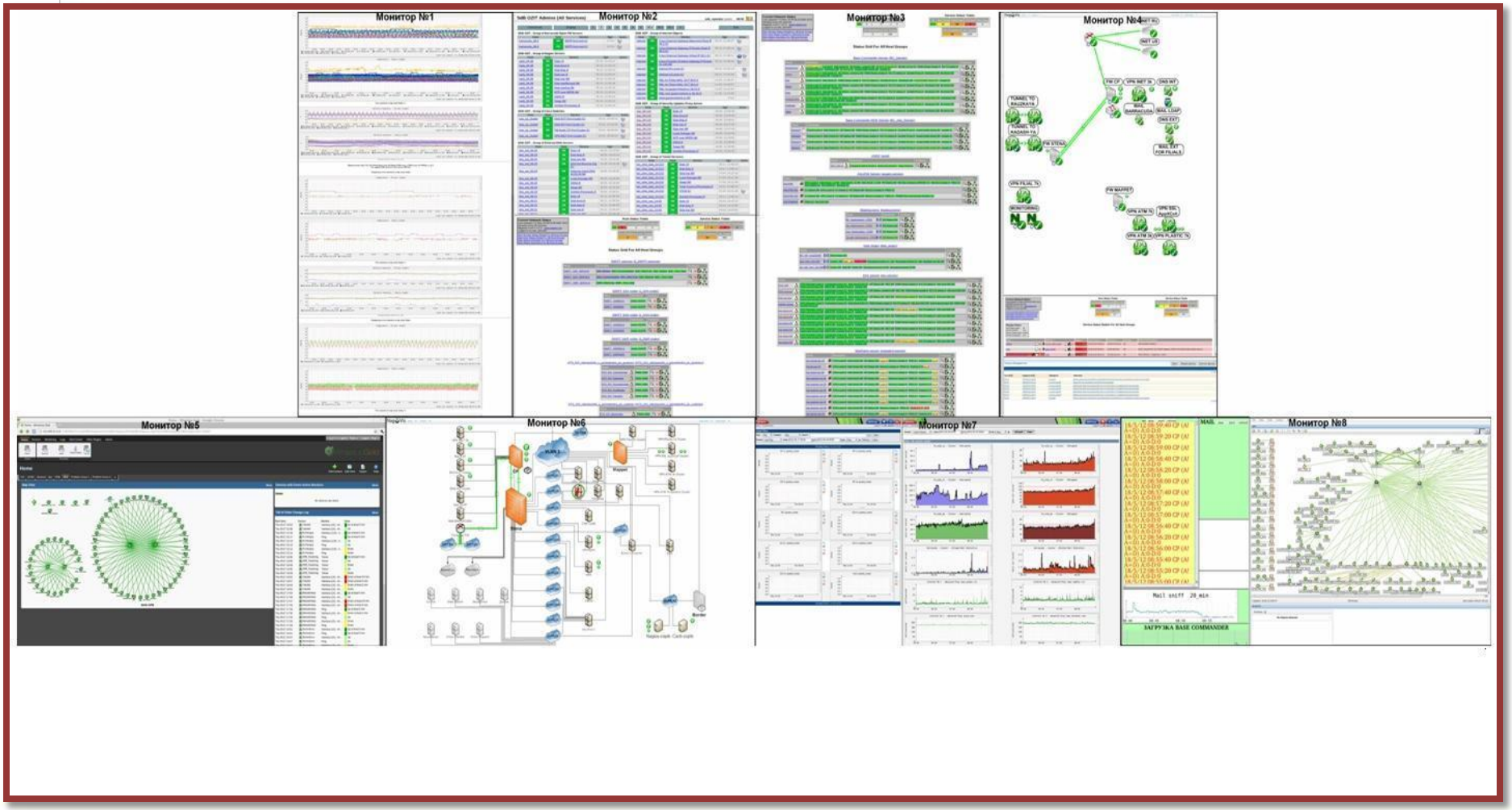
Осуществляется агрегирование всех правил в матрице разработанной на базе СТО БР, используя модель математической индукции.

уровень корреляции	состав корреляции	тип сформированной корреляции							пункты в таблице корреляций	кол-во правил корреляции	кол-во технологических правил	кол-во правил выявления инцидентов ИБ Д/Д/К
		TOC7	TOC6	TOC5	TOC4	TOC3	TOC2	TOC1				
	общее TOC4				4				5.			
Правила уровня TOC4 (Операционные Системы)	TOC3					3			5.1			
							2		5.1.1			
								1	5.1.1.1			
								1	5.1.2			
	TOC2						2		5.2			
								1	5.2.1			
	TOC1							1	5.3			
Правила уровня TOC3 (Сетевые сервисы)	общее TOC3					3			6.			
	TOC2						2		6.1			
								1	6.1.1			
	TOC1							1	6.2			
Правила уровня TOC2 (сетевые устройства)	общее TOC2						2		7.			
	TOC1							1	7.1			
Правила уровня TOC1 (физическое устройства)	общее TOC1							1	8.			

ГАЗПРОМБАНК

Технология работы

Осуществляется визуализации уровня оператора.

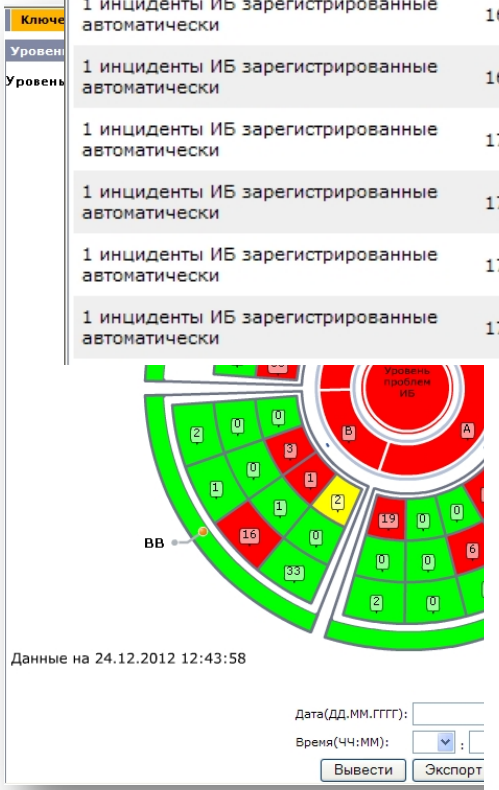


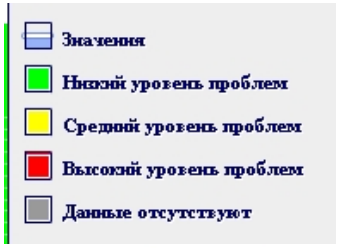
ГАЗПРОМБАНК

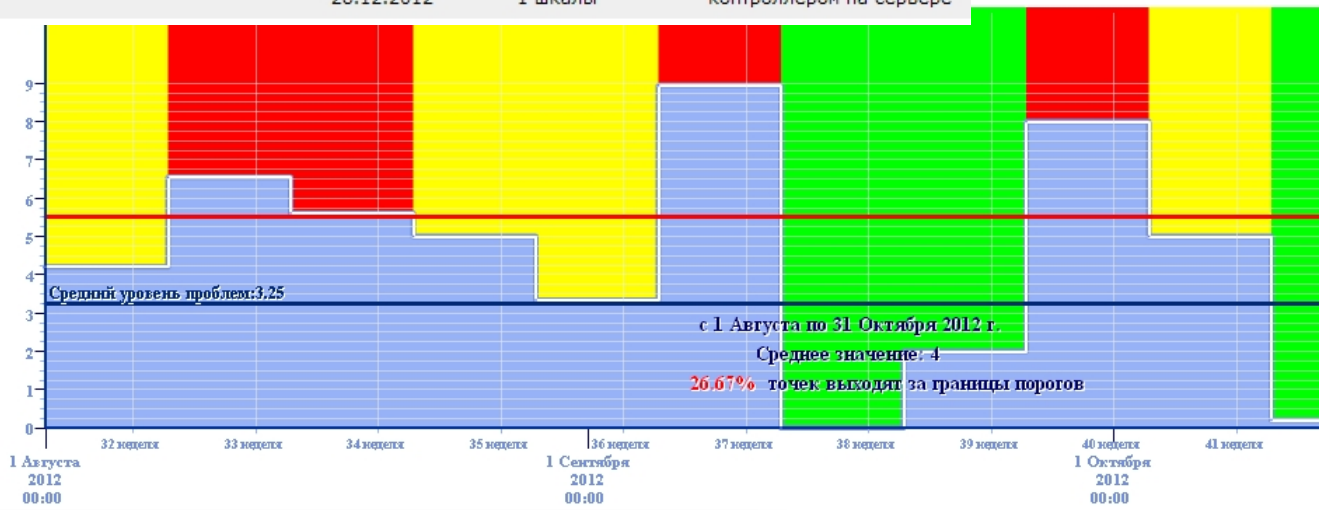
Технология работы

Осуществляется визуализации уровня руководителя.

Способ регистрации	Уникальный номер	Идентификатор в SD	Зарегистрирован	Приоритет	Описание
1 инциденты ИБ зарегистрированные автоматически	16741888168	89191	14:10:33 10.12.2012	3 средний — баллы 2 и 3 шкалы	Недоступность активного сетевого оборудования
1 инциденты ИБ зарегистрированные автоматически	16740955871	89190	14:10:33 10.12.2012	3 средний — баллы 2 и 3 шкалы	Недоступность активного сетевого оборудования
1 инциденты ИБ зарегистрированные автоматически	17492026399	89686	09:18:17 25.12.2012	1 очень низкий — балл 0 шкалы	Сбой в работе сервисов серверов СВОИ
1 инциденты ИБ зарегистрированные автоматически	17375394902	89607	10:59:47 22.12.2012	3 средний — баллы 2 и 3 шкалы	Недоступность активного сетевого оборудования
1 инциденты ИБ зарегистрированные автоматически	17375634666	89608	10:59:47 22.12.2012	3 средний — баллы 2 и 3 шкалы	Недоступность активного сетевого оборудования
1 инциденты ИБ зарегистрированные автоматически	17682474071	89783	11:16:44 28.12.2012	2 низкий — балл 1 шкалы	Проблемы с RAID контроллером на сервере







Технология работы

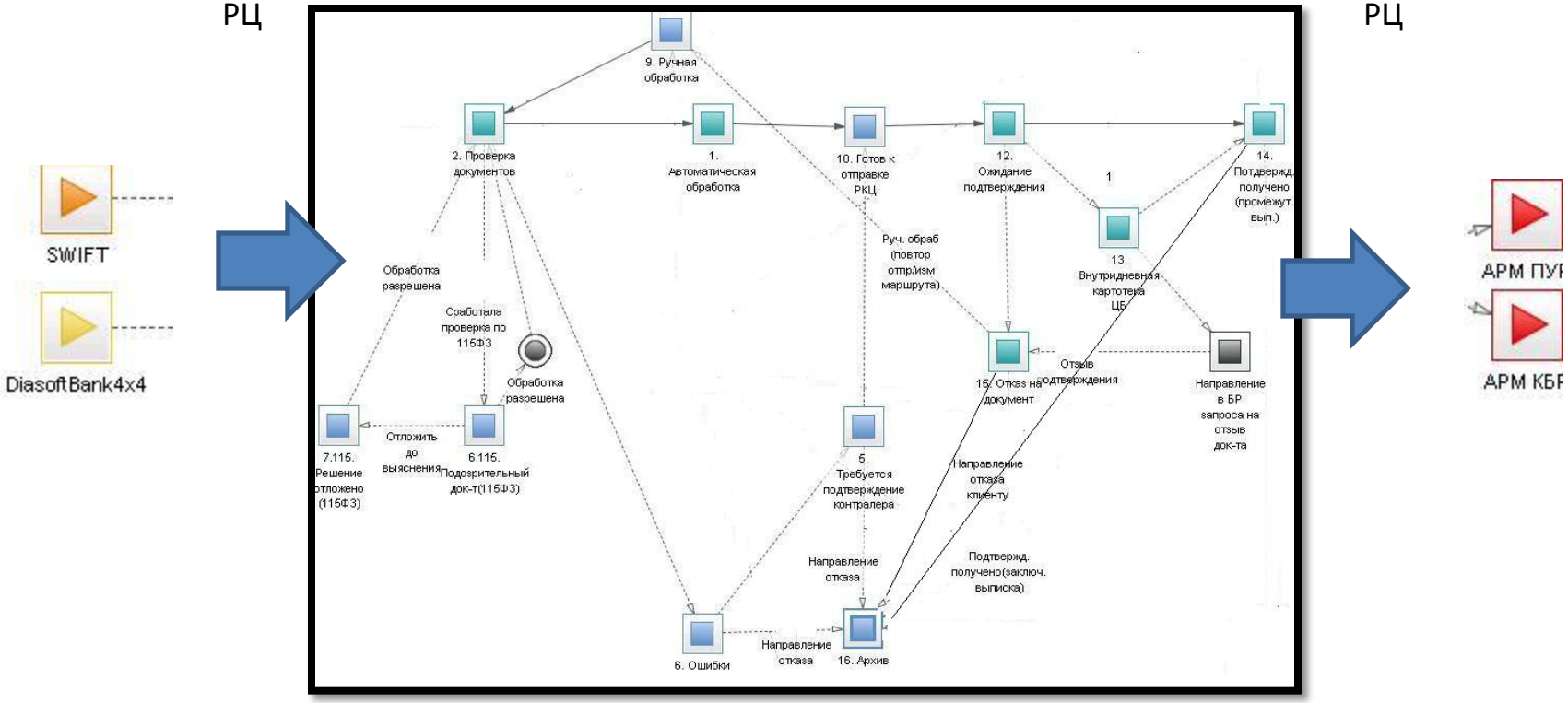
Осуществляется визуализации уровня технологического процесса на примере РЦ.

Входящая информация электронных расчетов для юридических лиц

Адаптеры РЦ

АС «РЦ»

Адаптеры РЦ



Технология работы

Осуществляется визуализации уровня технологического процесса на примере РЦ.

Исходящая информация электронных расчетов для юридических лиц

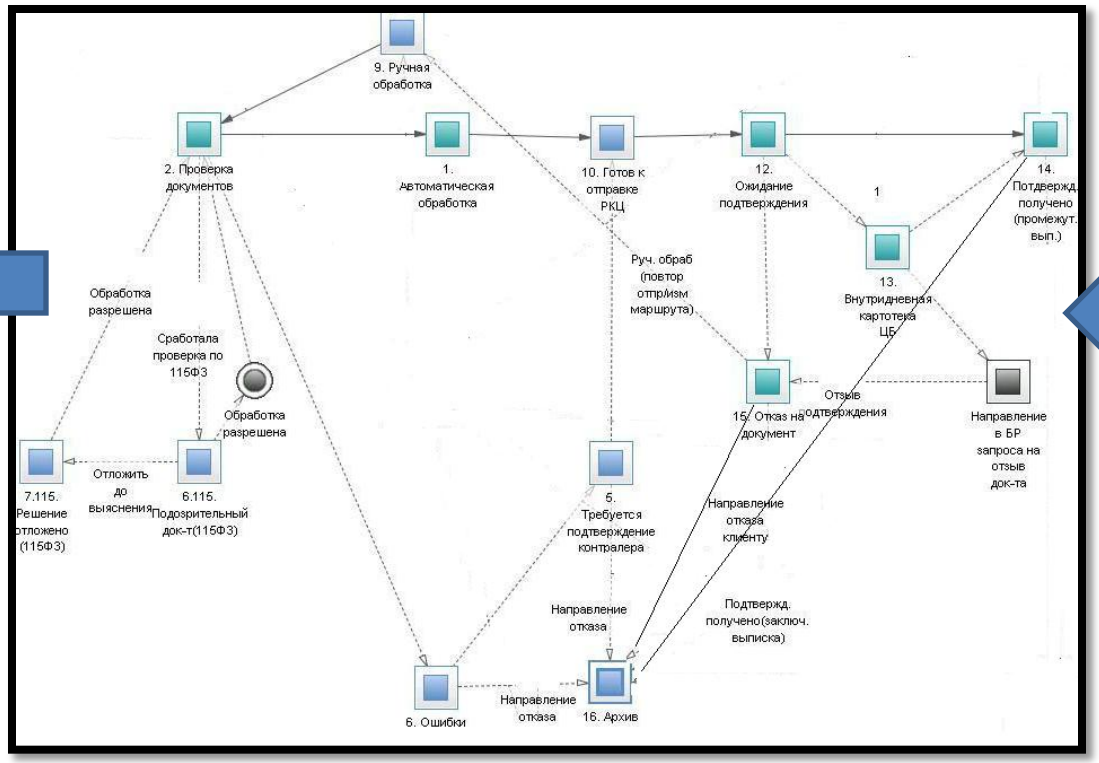
Адаптеры РЦ

АС «РЦ»

Адаптеры РЦ

SWIFT

DiasoftBank4x4



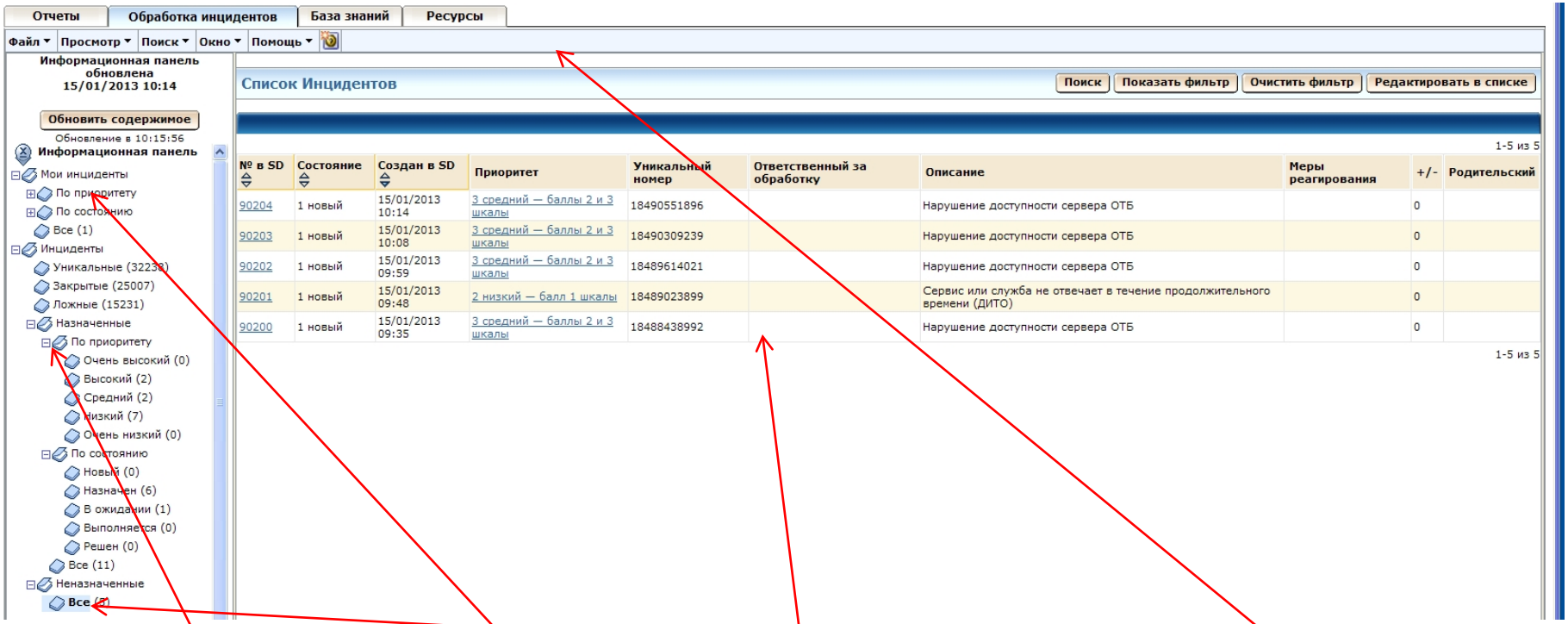
АРМ ПУР

АРМ КБР

ГАЗПРОМБАНК

Технология работы

Проведение расследования.



стандартные запросы дежурной смены

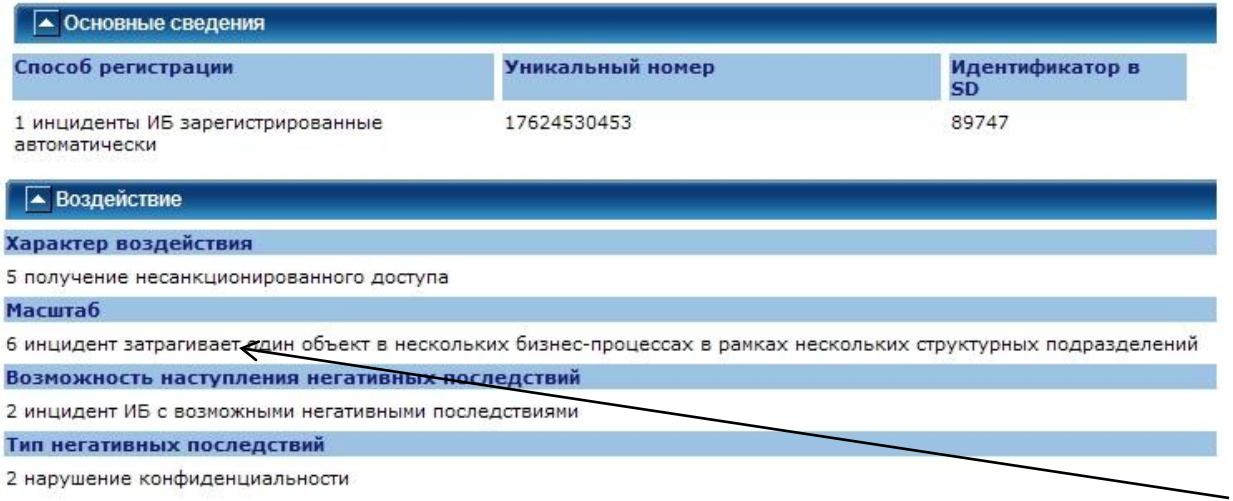
стандартные запросы дежурного оператора

новые инциденты

основная панель при классификации и расследовании инцидентов ИБ

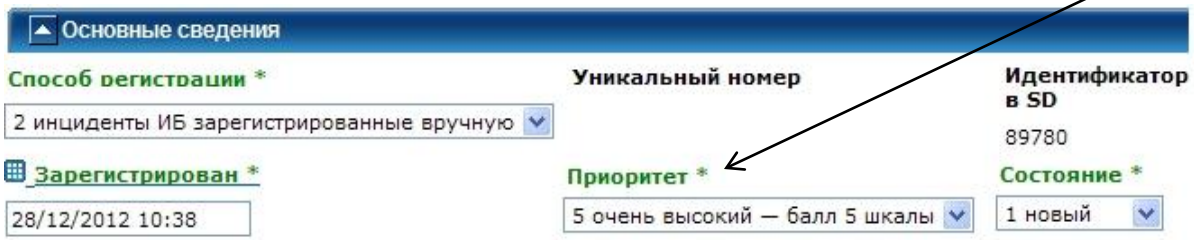
Технология работы

Проведение расследования.



параметры событий, заполняются автоматически

параметры событий, классифицируются



параметры событий, заполняются вручную

Технология работы

Проведение расследования.

Возможность оперативно (используя технологию DRILL DOWN) оценивать состояние инцидента ИБ

1 / (1) >>

Способ регистрации	Уникальный номер	Идентификатор в SD	Зарегистрирован	Приоритет	Описание
1 инциденты ИБ зарегистрированные автоматически	16741888168	89191	14:10:33 10.12.2012	3 средний — баллы 2 и 3 шкалы	Недоступность активного сетевого оборудования
1 инциденты ИБ зарегистрированные автоматически	16740955871	89190	14:10:33 10.12.2012	3 средний — баллы 2 и 3 шкалы	Недоступность активного сетевого оборудования
1 инциденты ИБ зарегистрированные автоматически	17492026399	89686	09:18:17 25.12.2012	1 очень низкий — балл 0 шкалы	Сбой в работе сервисов серверов СВОИ
1 инциденты ИБ зарегистрированные автоматически	17375394902	89607	10:59:47 22.12.2012	3 средний — баллы 2 и 3 шкалы	Недоступность активного сетевого оборудования
1 инциденты ИБ зарегистрированные автоматически	17375634666	89608	10:59:47 22.12.2012	3 средний — баллы 2 и 3 шкалы	Недоступность активного сетевого оборудования
1 инциденты ИБ зарегистрированные автоматически	17682474071	89783	11:16:44 28.12.2012	2 низкий — балл 1 шкалы	Проблемы с RAID контроллером на сервере

ГАЗПРОМБАНК

Технология работы

Контроль ИТ-ресурсов в соответствии с утвержденными профилями защиты в рамках предотвращения инцидентов ИБ.

ГАЗПРОМБАНК

Технология работы

Совершенствование внутренней нормативной базы.

Утверждены/идет разработка внутренних нормативных документов:

- Политика информационной безопасности;
- Частная Политика управления инцидентами ИБ;
- Регламент взаимодействия ССП в рамках мониторинга информационных программно-технических систем;
- Методические рекомендации по описанию инцидентов ИБ (идет разработка);
- Классификатор инцидентов, разработанный на основе СТО БР ИББС-1.0.-2010;
- Регламент сбора информации об инцидентах ИБ не автоматизированными средствами.

ГАЗПРОМБАНК

Результаты работы

В результате совершенствования системы менеджмента инцидентов информационной безопасности выполняются следующие задачи:

1. Совершенствуется нормативная база Банка в области менеджмента инцидентов ИБ;
2. Совершенствуются процедуры мониторинга ИБ (технические, организационные);
3. Совершенствуются механизмы обнаружения, анализа, сбора и управления инцидентов ИБ;
4. Совершенствуются правила выявления инцидентов ИБ (корреляции).

ГАЗПРОМБАНК

Результаты работы

1. Общее количество контролируемых АС - 84;
2. Настроено более 350 правил выявления инцидентов ИБ;
3. 16 СЗИ, являющиеся источником информации;
4. 29 утвержденных и контролируемых профилей защиты.
5. Ежедневное выявление более 20 инцидентов (из них около 5 уникальных)

За 2012 год выявлено и обработано более 18000 подозрений на инциденты ИБ (на основе 127 млрд. атомарных событий), из них подтверждено:

Сводная таблица инцидентов.

Уровни Типов Объектов Среды	Общее кол-во инцидентов	Родительских (уникальных) инцидентов	Дочерних инцидентов
ТОС6 (АС)	3120	156	2964
ТОС5 (СУБД)	104	52	52
ТОС4 (ОС)	2236	312	1924
ТОС3 (сетевой сервис)	468	364	104
ТОС2 (сетевое обор.)	312	52	260
ТОС1 (оборудование)	1986	1196	790
Всего инцидентов	**8226**	**2132**	**6094**

ГАЗПРОМБАНК

Перспективы развития

Обрабатываемые типы объектов среды (в соответствии со СТО БР):

1. физические объекты (линии связи, аппаратные средства и пр.);
2. сетевое оборудование (маршрутизаторы, коммутаторы, концентраторы и пр.);
3. сетевые приложения и сервисы;
4. операционные системы (ОС);
5. системы управления базами данных (СУБД);
6. банковские **технологические процессы** и приложения (модули банковских автоматизированных систем, банковские автоматизированные системы, **банковские информационные процессы и банковские платежные процессы**);

Новое СЗИ в качестве источника событий ИБ:

- **система контроля финансовых транзакций (Anti-Fraud).**

ГАЗПРОМБАНК

Спасибо за внимание

Вопросы ???

Контактная информация:

Егоркин Александр Викторович – ***начальник Департамента защиты информации ГПБ (ОАО)***

Телефон: +7 (495) 913-7933
E-mail: Alexander.Egorkin@gazprombank.ru