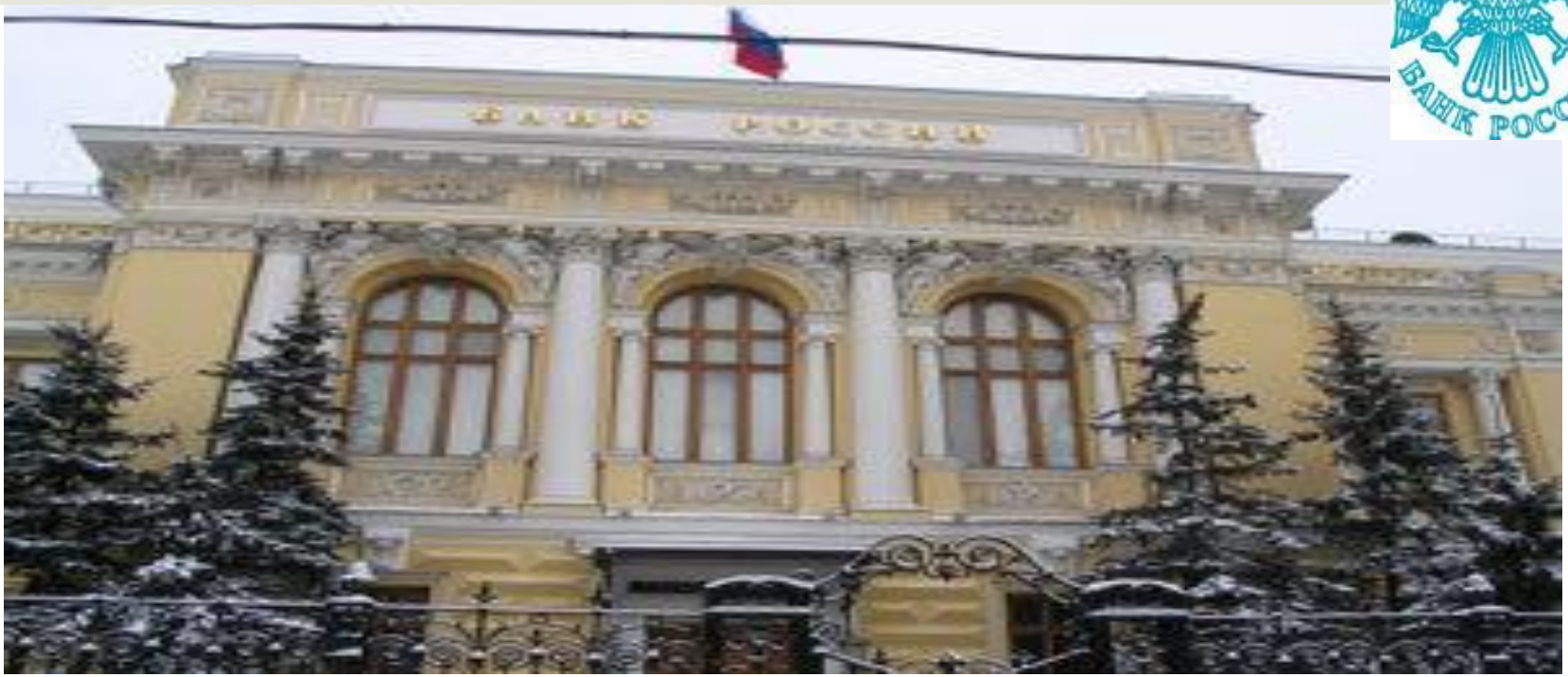
ВОЗРОЖДЕНИЕ БАНК

БАНК, КОТОРЫЙ ВСЕГДА С ТОБОЙ

Практические вопросы построения системы информационной безопасности многофилиального банка

Грициенко Андрей Александрович
Начальник Службы информационной безопасности Банка «Возрождение» (ОАО)

Требования к системе информационной безопасности Банка основываются на положениях Стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2008



«Политика информационной безопасности Банка «Возрождение» (ОАО)» (ПИБ-2008)

Устанавливает общие положения по обеспечению информационной безопасности в корпоративной информационной системе Открытого акционерного общества Банк “Возрождение”

Служба информационной безопасности

Удостоверяющий Центр Корпоративной Информационной Системы
Отдел внедрения и сопровождения систем обеспечения информационной безопасности
Отдел криптографической защиты информации
Отдел администраторов безопасности
Отдел информационной безопасности автоматизированных банковских систем
Отдел безопасности платежных систем
Отдел аудита и аттестации информационных систем

Администратор безопасности Банка

- Контроль выполнения установленных в Банке требований по обеспечению безопасности информации ограниченного доступа, предоставления пользователям полномочий по доступу к информационным активам (ресурсам) КИС Банка
- Регламентация действий и контроль администраторов информационных активов КИС Банка в части применения средств разграничения доступа и других средств обеспечения ИБ, а также средств антивирусной и антиспамовой защиты
- Оперативное и постоянное наблюдение, сбор, анализ и обработка данных под заданные цели, определяемые СМИБ КИС Банка, с использованием специализированных и штатных средств регистрации действий пользователей, процессов, процедур
- Согласование служебных записок (заявок и т.п.) на предоставление полномочий, копирование информации и т.д.

Центральный аппарат Банка – 4 администратора безопасности (посменно)

Филиал Банка – главный специалист по защите информации (зачастую – на внештатной основе)

Комплексные решения при построении системы ИБ или специализированные продукты?

- **На рынке преобладают решения специализирующиеся на отдельных направлениях ИБ**
- **Сложно получить продукт одинаково хорошо работающий в различных областях ИБ**
- **Комплексные решения применимы в основном для небольших компаний**

При реализации требований по обеспечению информационной безопасности в корпоративной информационной системе Банка применяются продукты и решения компаний, занимающих лидирующее положение на рынке решений в области ИБ

Обеспечение информационной безопасности при использовании средств электронной почты

Требования к системе:

- **Контроль за содержимым всей почтовой переписки в Банке**
- **Хранилище исходящей переписки с возможностью восстановления и сроком хранения данных до 5 лет**
- **Централизованное хранение и управление в условиях разветвленной структуры Банка**
- **Оперативный и гибкий доступ к информации в хранилище**
- **Выявление и пресечение фактов нарушения Закона «О персональных данных»**

InfoWatch Traffic Monitor

- **С защищенным хранилищем корпоративного масштаба**
- **С возможностью восстановления данных**
- **С возможностью настройки длительности хранения (на любой срок)**
- **С защитой только что созданных документов, без необходимости предварительного индексирования**
- **С гибкими настройками политик безопасности**
- **С возможностью интеграции с другими решениями**
- **Полный контроль за перепиской с доказательной базой для расследования инцидентов**

Преимущества использования

- **Известный производитель, с успешным опытом внедрения решений в крупнейших банках России**
- **100% российская компания**
- **Быстрое внедрение**
- **Работа Traffic Monitor абсолютно прозрачна и настройки могу быть изменены администратором безопасности**
- **Высокая производительность**
- **Полный и централизованный контроль всей переписки**
- **Наличие сертификата ФСТЭК России**

Обеспечение информационной безопасности при использовании ресурсов сети Интернет

Требования к системе:

- **Система защиты корпоративной информационной системы, работающая на единой интегрированной технологической платформе**
- **Полное инспектирование контента web-страницы**
- **Гибкая архитектура, возможность автоматической установки и обновления программного обеспечения**
- **Самообучение и блокировка нежелательных web-сайтов**
- **Фильтрация приложений для адресного блокирования Интернет-пейджеров (IM), клиентов файлообменных сетей (P2P), неавторизованного туннелирования**
- **Высокая пропускная способность**

Проактивная система контентной фильтрации трафика Aladdin eSafe Web

Помимо защиты от вирусов, шпионских приложений и URL-фильтрации система предоставляет средства для реализации безопасных политик использования Интернет-ресурсов путем:

- **"Вырезания" вредоносных и подозрительных скриптов из web-страниц, web-почты, тела email**
- **Блокирования всех скриптовых вирусов и эксплойтов.**
- **Блокирования известных и неизвестных на момент проверки HTML- и HTTP-эксплойтов**

Дополнительные опции:

- **Удаление тэгов ActiveX**
- **Возможность разрешить выполнение только предопределенным доверенным ActiveX объектам**
- **Возможность разрешить выполнение только предустановленным доверенным ActiveX объектам**
- **Блокирование Java-апплетов**
- **Запрет cookie-файлов**
- **Блокирование страниц, содержащих определенные ключевые слова**
- **Сканирование зашифрованного контента при доступе к web-странице по SSL**

Преимущества использования

- **Высокая производительность и масштабируемость**
- **Сканирование Web-трафика в режиме реального времени**
- **Простота конфигурирования и управления**
- **Балансировка нагрузки**
- **Успешный опыт внедрения в крупных компаниях**
- **Наличие сертификата ФСТЭК России**

Мониторинг и управление событиями ИБ

Требования к системе:

- **Способность получать и обрабатывать данные с огромного количества программно-аппаратных комплексов сети (серверов, межсетевых экранов и др.) различных вендоров**
- **Предоставление результатов анализа событий в режиме реального времени**
- **Поддержка различных методов обнаружения атак**
- **Возможность создания собственных правил корреляции**
- **Централизованное хранение данных, поступающих от всех систем**
- **Гибкая схема создания отчетов**
- **Маштабируемость**

Система управления событиями информационной безопасности ArcSight ESM

Система осуществляет:

- **Сбор информации о событиях с различных устройств обеспечения информационной безопасности и сетевых устройств**
- **Визуализацию событий на карте сети в режиме реального времени**
- **Поддержку сигнатурных и «поведенческих» методов обнаружения аномалий и атак**
- **Возможность создания собственных правил корреляции**
- **Возможность управления активными сетевыми устройствами в целях блокирования вредоносного трафика**
- **Разделение полномочий по управлению**
- **Поддержку протоколов сбора событий Syslog, SNMP, RDEP, SDEE**
- **Временные метки событий**
- **Уведомление об обнаруженных проблемах по e-mail, SNMP, syslog**
- **Управление через графический web-интерфейс, Java-интерфейс и др.**

Источниками событий могут быть практически все типы сетевого оборудования, средства обеспечения информационной безопасности приложений

Преимущества использования

- **Обзор данных в реальном режиме времени от всех ИС**
- **Централизованное хранение данных, поступающих от всех ИС**
- **Классификация угроз по уровням опасности для выявления реальных и игнорирования ложных**
- **Способность агрегировать данные с большого количества программно-аппаратных элементов сети (серверов, межсетевых экранов и др.) различных вендоров**
- **Мощная база предустановленных правил корреляции событий безопасности, существенно упрощающая администрирование системы**
- **Анализ данных по многим нарушениям безопасности: от атак до корпоративных политик**
- **Проверка системы безопасности на соответствие стандартам (ISO 27001, PCI DSS и др.), а также другим нормативным и законодательным актам**
- **Широкие и гибкие возможности мониторинга распределенных систем большого масштаба**
- **Наличие сертификата ФСТЭК России**

Заключение

Внедрение указанных средств в рамках системы информационной безопасности КИС Банка оказалось практически полезным для систематизации и упорядочения деятельности Службы ИБ Банка по обеспечению информационной безопасности, что в конечном итоге способствует снижению операционного риска в процессе основной деятельности Банка

ВОЗРОЖДЕНИЕ БАНК

БАНК, КОТОРЫЙ ВСЕГДА С ТОБОЙ

Спасибо за внимание!

Грициенко Андрей Александрович
Начальник Службы информационной безопасности Банка «Возрождение» (ОАО)