Системы криптографической защиты информации

Опыт внедрения ЦСК в банках Украины

Ковтун Владислав
Компания «Сайфер»

Специфика банка

Банк является сложной информационно-телекоммуникационной системой, которая:

- Множество систем
- Интеграция систем между собой
- Разные поставщики и разработчики систем
- Новые и старые решения/технологии
- Необходимость иметь доступ к историческим данным
- Разные требования к средствам защиты (КЗИ) для различных систем

Достаточно ли внимание к КЗИ?

- **Бизнес-главное, а защита - потом**
- Менеджмент ИТ и ИТ-безопасности предлагает, а бизнес-менеджмент - отклоняет
- Разработчики Бизнес-систем уделяют недостаточно внимания КЗИ
- **НБУ, как регулятор находится на пути регулирования вопросов КЗИ в банковских системах**
- Top-менеджмент уделяет внимание КЗИ, только когда **банк обязан**
- Низкий уровень зрелости ИТ инфраструктуры и Top-менеджмента
- Сложная финансовая ситуация в стране/банке
- Есть более важные задачи перед банком/ИТ-подразделением
- О защите вспоминают **по факту** …

Банковские системы

Важные системы банка требующие КЗИ:

- ДБО (ИБ/КБ/WБ) для физлиц/юрлиц/МСБ
- АБС
- ВПС
- Процессинговые центры платежных карт
- Межбанковские платежные системы
- Front-офисные системы
- СЭДО
- Другие

Средства КЗИ в банках

- Современные решения ЦСК 3G – X.509 (ЦСК-1.X, Шифр-X.509, Вега 2.0, CryptoKDC)
- Устаревшие решения ЦСК 2G (Шифр-PKI, Вега, Щит)
- Уже встроенные в банковские системы, от разработчиков банковских систем (Bifit, ELPay, CS iFOBS и другие)
- Собственные разработки банков (ПУМБ, Проминвестбанк и другие)
- Решения от НБУ (например ЦСК НБУ в рамках СЭП)

Внедрение новых средств КЗИ

Отсутствие интереса:

- Стоимость интеграции с существующими банковскими системами
- Стоимость внедрения (изменение бизнес процессов/организационно-штатной структуры/обновления/оборудования)
- Сложность современных средств КЗИ
- Продолжительность интеграции, внедрения и последующей миграции существующих систем
- Необходимость непрерывного обновления

Мы должны дать заказчику не то, что он хочет, а то, что ему нужно!

Конструктор Яковлев А.С.

Пути решения для банков

- Не ждать регулятора, а обращаться к нему за разъяснениями
- Планировать развитие сотрудников, ИТ-инфраструктуры и безопасности (КЗИ)
- Активно доносить до руководства необходимость развития не только бизнес систем/ИТС, но средств КЗИ к ним указывая возможные риски
- Вовлекать в процесс профессионалов в области КЗИ (Сайфер, ИИТ, Автор и др.)
- «Учиться, учиться и еще раз учиться!»
- Дорогу осилит идущий …

Сложности внедрения

- Отсутствие единых координаторов по каждому направлению (бизнес/ИТ/безопасность)
- Высокая текучесть кадров
- Разделение между потребителями, внедренцами и эксплуататорами
- Недостаточное количество ИТ-специалистов
- Необходимость в узкопрофильной (КЗИ) подготовки специалистов
- Особые требования от бизнеса к процессам

Подходы к успешному внедрению

- Доступность и удобство системы
- Автоматизация рутинных процессов
- Проведение обучения будущих пользователей
- Вовлечение в процесс развертывания будущих сотрудников ЦСК
- Детальные руководства по развертыванию и эксплуатации
- Оперативная дистанционна поддержка, с возможностью выезда на место (Киев)

Подходы к успешной интеграции

- Наличие библиотек полного цикла, для интеграции с банковскими системами
- Разработка спецификаций по интеграции с различными системами (передача знаний)
- Знания специфики банковских систем
- Удобный набор инструментов для интеграции в банковские системы и тестовый полигон
- Сопровождение работ по интеграции
- Непрерывное совершенствование библиотек/технологий/документации нормативным требованиям

Преимущества ЦСК 3G

- Универсальность и гибкость, обеспечивает КЗИ в любых АБС, ДБО, СЭДО и других системах
- Современность, эксплуатация продолжительное время
- Возможность создания ЦСК, который может быть зарегистрирован/аккредитован в Удостоверяющем центре НБУ или ЦУО Украины
- Повышенная надежность и безопасность обслуживания удаленных пользователей, посредством сервисов работающих в интерактивном режиме (OCSP, TSP, LDAP), уменьшая вероятность «коллизий»
- Упрощается порядок смены ключей клиентов и работников банка: смена происходит на рабочем месте клиента, без необходимости посещения банка

Преимущества ЦСК 3G

- Упрощение порядка регистрации (выдачи ключей) клиентам и работникам банка: клиент посетит отделение 1-2 раза, вместо 3-х
- Единая система управления ключами и сертификатами для АБС, ДБО, СЭДО, платежных систем и т.д.
- Поддержка стандартов ЭЦП ДСТУ 4145-2002/RSA
- Реализация требований семейства стандартов X.509 в полном объеме (полноценная ИОК)
- Ориентация на обслуживание пользователей в интерактивном режиме
- Повышается защита и надежность хранения ключевой информации: работа с защищенными носителями (ключ хранится внутри защищенного устройства)

Преимущества 3G

- Адаптация ЦСК под существующие и будущие бизнес-процессы банка
- Упорядочивание процессов защиты информации (не только КЗИ), что существенно снижает риски
- Возможность развивать собственную ИТС, посредством встраивания стандартизированных библиотек/агентов
- Возможность использования единых сервисов аутентификации для множества систем, с единым управлением доступом
- Централизованное обновление, в том числе и на соответствие нормативным документам

Продукты нашей компании

Система криптографической защиты информации **«Шифр-X.509»** позволяет построить ЦСК в банке и в дальнейшем успешно пройти процедуру регистрации или аккредитации.

Отличается:

- Разумной ценой
- Уменьшенной стоимостью владения
- Высокой гибкостью и масштабируемостью
- Легкой интеграцией с другими банковскими системами
- Позволяет обслуживать более 1 млн сертификатов без существенных требований к оборудованию и БД
- Возможность построения ЦСК в одном и нескольких ЦОД

Спасибо за внимание

Компания «Сайфер»

г. Киев ул. Нагорная д.25-27

Тел.: (044) 484-46-12

(044) 484-46-17

E-mail: vk@cipher.kiev.ua

WWW: cipher.kiev.ua

Вопросы к Регулятору

- Допустимые алгоритмы и форматы данных?
- Когда планируется избавиться от ГОСТ34.310-95??
- Легитимность международных алгоритмов (RSA/DSA/ECDSA+SHA1/2/3+AES/TDES)?
- Длины ключей? Требуемые уровни защиты для банковских систем?
- Инфраструктура открытых ключей?
- Необходимость в построении КСЗИ и/или ISO 27001+27001 для аккредитации?

Архитектура