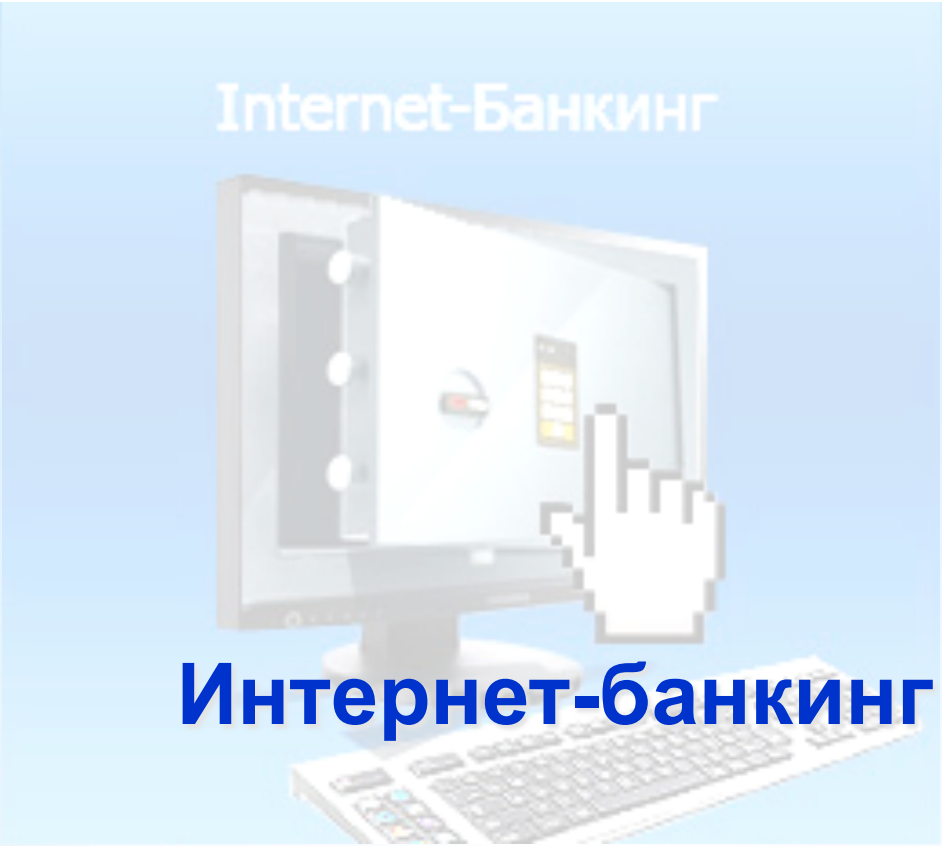
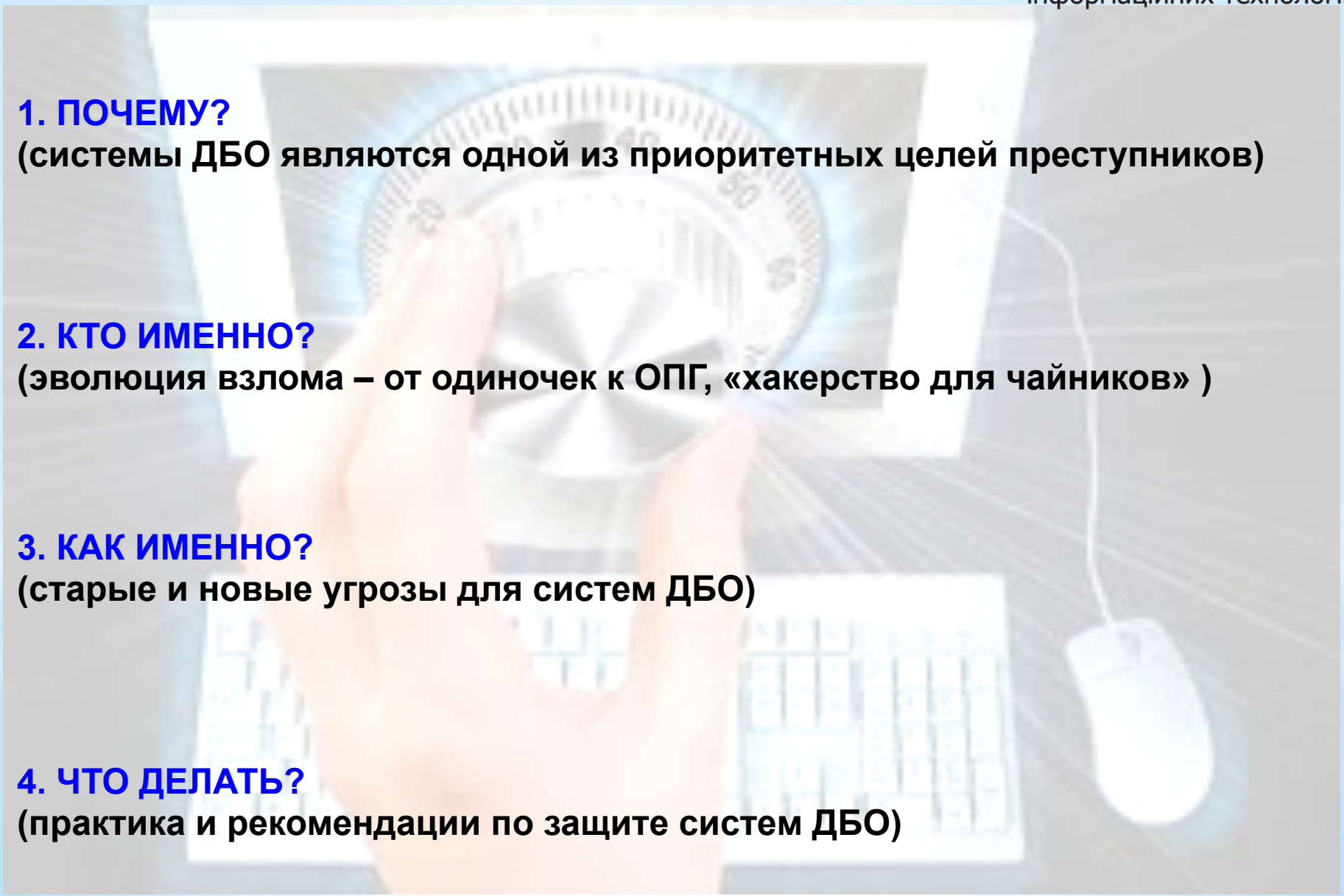


Интернет-банкинг

Современные угрозы безопасности и практика защиты от них

Олег Балаба
Менеджер по продажам ООО ”CBIT IT”
Киев, конференция ”Банк Online 2012”



1. ПОЧЕМУ?
(системы ДБО являются одной из приоритетных целей преступников)

2. КТО ИМЕННО?
(эволюция взлома – от одиночек к ОПГ, «хакерство для чайников»)

3. КАК ИМЕННО?
(старые и новые угрозы для систем ДБО)

4. ЧТО ДЕЛАТЬ?
(практика и рекомендации по защите систем ДБО)

1. ПОЧЕМУ?

(системы ДБО я
ц

Когда Ал

нег,
одать

(практически)

(сейчас) несо

2. КТО ИМЕННО?
(эволюция взлома – от одиночек к ОПГ, «хакерство для «чайников»)

(в основном) ради интереса

(в основном) ради навредить, не получив прибыли

(в основном) для получения прибыли

Организованные преступные сообщества с распределением обязанностей

Бот-сети, использование для взлома «облачных» технологий

- Конструктор вирусов с годовой подпиской
- Сканеры уязвимостей
- Общедоступная литература и ПО

Изначально хакерами называли программистов, которые исправляли ошибки в программном обеспечении каким-либо быстрым и далеко не всегда элегантным (в контексте используемых в программе стиля программирования и ее общей структуры, дизайна интерфейсов) или профессиональным способом; такие правки ассоциировались с «топорной работой» из-за их грубости, отсюда и произошло название «хакер»

3. КАК ИМЕННО?
(старые и новые угрозы для систем ДБО)

4. ЧТО ДЕЛАТЬ?
(практика и рекомендации по защите систем ДБО)

3. КАК ИМЕННО?
4. ЧТО ДЕЛАТЬ?

(старые и новые угрозы для систем интернет-банкинга)		(практика и рекомендации по защите систем интернет-банкинга)
Кража паролей пользователей	65-75%	Одноразовые пароли для входа в систему
Кража ключей ЭЦП пользователей		Использование защищенных носителей ЭЦП
Удаленное подключение к рабочему месту пользователя	15-17%	Использование одноразовых паролей для подтверждения платежа
Проброс USB-порта, к которому подключен токен	3-5%	Применение электронной подписи, основанной на реквизитах платежного документа
Подмена платежного документа	1-2%	Использование защищенной программной среды

Взаимодействие в системах интернет-банкинга
(аспекты, которые сегодня останутся «за кадром»)

iT CBIT
інформаційних технологій

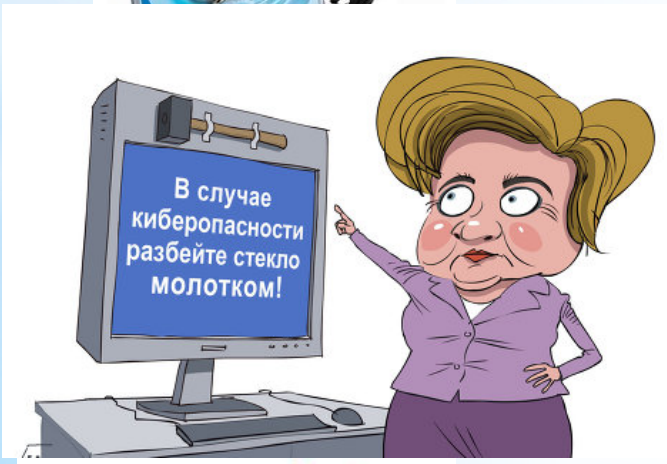
Клиент банка

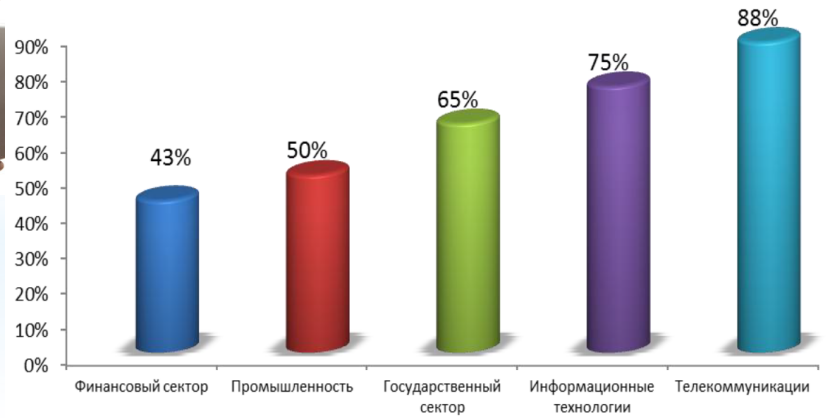
Интернет

Система интернет-банкинга

Защита рабочих станций (End-Point Security)

Защита на уровне сети и приложений





Статистика уязвимостей веб-приложений за 2010—2011 годы (c) Positive Technologies

Взаимодействие в системах интернет-банкинга
(защита на стороне клиента)

Клиент банка

Одноразовые пароли для входа в систему

Использование защищенных носителей ЭЦП

Использование одноразовых паролей для подтверждения платежа

Применение электронной подписи, основанной на реквизитах платежного документа

Возможно предотвратить до 90% атак на пользователя интернет-банкинга

Взаимодействие в системах интернет-банкинга
(защита на стороне системы)

CBIT
інформаційних технологій

Поддельный платежный документ

Отправка клиенту сообщений (SMS, E-mail) о платежах с его банковского счета

Использование системы мониторинга транзакций по банковскому счету клиента (Fraud Monitoring)

Предоставление клиенту различных возможностей в системе интернет-банкинга в зависимости от степени его защиты

RSA® Transaction Monitoring

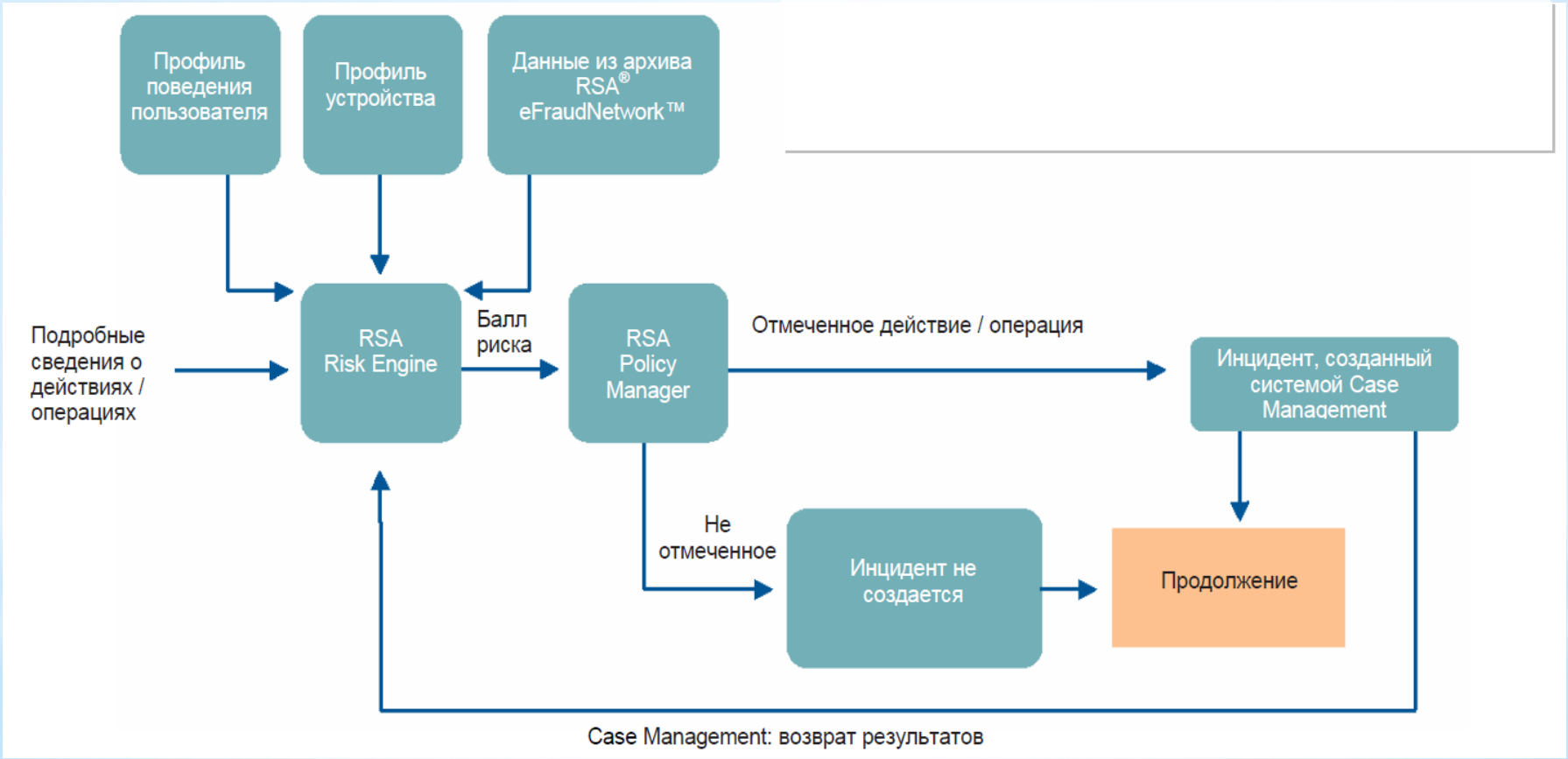
- снижение числа мошенничеств на 96%
- коэффициент ложных срабатываний 1:880
- мониторинг, обнаружение, противодействие, самообучение

Предоставление клиенту различных возможностей в системе интернет-банкинга в зависимости от степени его защиты

СВІТ інформаційних технологій

Уровень защиты	Возможности в системе интернет-банкинга	
	Юридические лица	Физические лица
Постоянный логин и постоянный пароль	Проверить остаток на счете	Просмотреть выписку по счету, сделать платеж по известным реквизитам
Постоянный логин и одноразовый пароль (в SMS)	Просмотреть выписку и движения по счету	Сделать платеж по произвольным реквизитам на сумму до 2 000 грн.
Постоянный логин и одноразовый пароль (аппаратный генератор)	Просмотреть выписку и движения по счету	Сделать платеж по произвольным реквизитам на сумму до 5 000 грн.
Логин, одноразовый пароль (аппаратный), ЭЦП на обычном носителе	Просмотреть выписку по счету, сделать платеж до 50 000 грн.	Сделать платеж по произвольным реквизитам на сумму до 10 000 грн.
Логин, одноразовый пароль (аппаратный), ЭЦП на защищенном носителе	Просмотреть выписку по счету, сделать платеж до 500 000 грн.	Без ограничений
Логин, одноразовый пароль, ЭЦП на защищенном носителе, подтверждение платежа	Без ограничений	Без ограничений

Система мониторинга транзакций по банковскому счету клиента (на примере RSA® Transaction Monitoring)



Одноразовые пароли и электронная подпись на украинском рынке услуг интернет-банкинга

iT CBIT інформаційних технологій

- Укрэксимбанк
- Укрсиббанк
- Акта Банк
- Банк Пивденный
- Таскоммерцбанк (Сведбанк)
- Надра Банк
- СЕБ Банк
- Авант Банк

- ОТР банк

RSA SECURITY

- Раффайзен Банк Аваль

gemalto security to be free

VASCO THE AUTHENTICATION COMPANY

- компания CS
- компания Бифит

- компания CS
- компания Lime Systems

VASCO – Более 80 видов продуктов

CBIT
інформаційних технологій

Защищенные носители ЭЦП на украинском рынке услуг интернет-банкинга

- Райффайзен Банк Аваль
- Сбербанк России
- Проминвестбанк
- Альфа Банк
- Укрэксимбанк
- Надра Банк
- Банк Крещатик
- Банк Кипра
- Сведбанк
- Укрсоцбанк
- Правекс Банк
- Эрсте Банк
- ПУМБ
- Энергобанк

SafeNet

THE DATA PROTECTION COMPANY

- компания CS
- компания Сайфер
- компания НОКК

ЕКСПЕРТНИЙ ВИСНОВОК

Прим. № 1

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Прим. № 1

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Прим. № 1

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

01034, м. Київ, вул. Паторжинського, 5/7,
тел. (044) 281-90-10, факс: (044) 226-26-83, e-mail: info@dsszzi.gov.ua

05.09.2012 № 05/02/02-3803

ЕКСПЕРТНИЙ ВИСНОВОК

Виданий: Товариству з обмеженою відповідальністю "СЕРВІСЛОГІСТІК" (код ЄДРПОУ 37500361)

на підставі рішення Експертної комісії з питань проведення державної експертизи в сфері криптографічного захисту інформації Державної служби спеціального зв'язку та захисту інформації України, протокол від 05.09.2012 № 94.

Об'єкт експертизи: Вироби SafeNet eToken 5000 (eToken 4000), SafeNet iKey 4000 (iKey 4000).

Розроблений (виготовлений): SafeNet Inc., Ізраїль.

Експертний заклад: Інститут спеціального зв'язку та захисту інформації НТУУ "КПІ" (код ЄДРПОУ 34979237).

Висновки:
1. В об'єкті експертизи алгоритм шифрування відповідає вимогам алгоритму TDES, визначеному в п. 4.1 ISO/IEC 18033-3:2010.
2. В об'єкті експертизи алгоритм шифрування відповідає вимогам алгоритму AES, визначеному в п. 5.1 ISO/IEC 18033-3:2010.
3. В об'єкті експертизи алгоритм шифрування та накладання електронного цифрового підпису відповідає вимогам алгоритму RSA, визначеному в IETF RSA 3447.
4. В об'єкті експертизи алгоритм гешування відповідає вимогам алгоритму SHA-1, визначеному в розділі 9 ДСТУ ISO/IEC 10118-3:2005.

Особливі умови (рекомендації): Дія експертного висновку поширюється на зразки об'єктів експертизи SafeNet eToken 5000 (eToken 4000) (№ 90516576), SafeNet iKey 4000 (iKey 4000) (№ 90516576).

Термін дії експертного висновку: до 05.09.2015.

Перший заступник Голови Служби О.Г. Цуркан

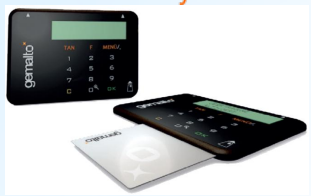
М.П.

ООО «СВІТ ІТ»
(044) 457-63-22
svit-it.com.ua

Спасибо!

СВІТ
інформаційних технологій

gemalto
security to be free



RSA
SECURITY

VASCO
THE AUTHENTICATION COMPANY

SafeNet

THE
DATA
PROTECTION
COMPANY