Региональный семинар МСЭ для стран СНГ

«Развитие электронного правительства как одно из условий интеграции в глобальное информационное общество»

г. Москва, Российская Федерация, 25-27 ноября 2013 года

Криптографическая система обеспечения безопасности государственной информационной инфраструктуры и цифрового контента

Маслов Юрий
Коммерческий директор
ООО «КРИПТО-ПРО»

Криптографические алгоритмы и стандарты

Алгоритм выработки значения хэш-функции

Обозначение ГОСТ	**ГОСТ Р 34.11-94**
Наименование на русском языке	Информационная технология. Криптографическая защита информации. Функция хэширования
Наименование на английском языке	Information technology. Cryptographic data security. Hash function
Дата введения в действие	01.01.1995
Обозначение ГОСТ	**ГОСТ Р 34.11-2012**
Наименование на русском языке	Информационная технология. Криптографическая защита информации. Функция хэширования
Наименование на английском языке	Information technology. Cryptographic data security. Hash function
Дата введения в действие	01.01.2013

Криптографические алгоритмы и стандарты

Алгоритм формирования и проверки ЭЦП

Обозначение ГОСТ	**ГОСТ Р 34.10-2001**
Наименование на русском языке	Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи
Наименование на английском языке	Information technology. Cryptographic data security. Signature and verification processes of [electronic] digital signature
Дата введения в действие	01.07.2002
Обозначение ГОСТ	**ГОСТ Р 34.10-2012**
Наименование на русском языке	Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи
Наименование на английском языке	Information technology. Cryptographic data security. Signature and verification processes of [electronic] digital signature
Дата введения в действие	01.01.2013

Криптографические алгоритмы и стандарты

Алгоритм зашифрования/расшифрования данных и вычисление имитовставки

Обозначение ГОСТ	**ГОСТ 28147-89**
Наименование на русском языке	Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования
Наименование на английском языке	
Дата введения в действие	30.06.1990

Требования к криптографическим средствам

СИСТЕМА
сертификации средств криптографической защиты информации
Регистрационный номер Госстандарта России
РОСС RU.0001.030001 от 15.11.93

- Требования ФСБ России к шифровальным (криптографическим) средствам (закрытый документ)
- Требования ФСБ России к информационной безопасности удостоверяющих центров систем электронного документооборота (закрытый документ)
- Требования к средствам электронной подписи (утверждены приказом ФСБ России от 27 декабря 2011 года № 796)
- Требования к средствам удостоверяющего центра(утверждены приказом ФСБ России от 27 декабря 2011 года № 796)

Реализация криптографических средств

Разработка криптографических средств:

- ❑ осуществляется хозяйствующими субъектами по техническому заданию согласованному с ФСБ России
- ❑ осуществляется в форме программных библиотек, программно-аппаратных компонент или законченных программных и/или программно-аппаратных комплексов

Сертификация криптографических средств :

- ❑ система добровольной сертификации
- ❑ сертификационные испытания проводятся аккредитованными ФСБ России лабораториями

Перечень сертифицированных криптографических средств публикуется:

http://clsz.fsb.ru/certification.htm

Порядок применения криптографических средств (общего характера)

- Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утверждённое приказом ФСБ России от 9 февраля 2005 г. N 66

- «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденные руководством 8 Центра ФСБ России 21.02.2008 № 149/54-144

- «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622.

Особенности применения криптографических средств

- Совместимость криптографических средств только на уровне реализации криптографических алгоритмов
- Отсутствует стандартизация криптографических сообщений (подписанного сообщения, шифрованного сообщения и т.д.)
- Отсутствует стандартизация криптографических протоколов

Применение криптографических средств в системах государственной информационной инфраструктуры

Для обеспечения использования электронных подписей:

- ❑ при предоставлении государственных или муниципальных услуг и исполнении государственных или муниципальных функций
- ❑ при межведомственном взаимодействии, осуществляемом в электронном виде
- ❑ в системах электронного документооборота органов власти и органов местного самоуправления

Для обеспечения защиты информации путём шифрования:

- ❑ при предоставлении государственных или муниципальных услуг и исполнении государственных или муниципальных функций
- ❑ при межведомственном взаимодействии, осуществляемом в электронном виде
- ❑ при организации доступа к государственным информационным ресурсам

Для обеспечения идентификации и аутентификации:

- ❑ при предоставлении государственных или муниципальных услуг и исполнении государственных или муниципальных функций
- ❑ при межведомственном взаимодействии, осуществляемом в электронном виде

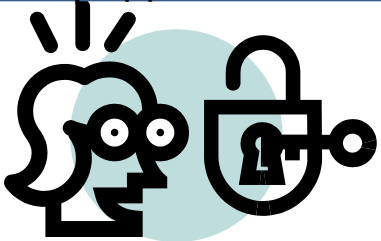
PKI – одна из основных технологий в применении криптографических средств

МИНКОМСВЯЗЬ РОССИИ

Система аккредитованных УЦ

свыше 300

Юридические и физические лица



свыше 3 млн

Государственные информационные системы

Система аккредитованных УЦ

МИНКОМСВЯЗЬ РОССИИ

Создана для обеспечения применения квалифицированной электронной подписи

Действует на основании:

1. Федерального закона от 6 апреля 2011 года N 63-ФЗ «Об электронной подписи»
2. Приказа Минкомсвязи России от 23.11.2011 №320 «Об аккредитации удостоверяющих центров»
3. Приказа Минкомсвязи России от 13.04.2012 №108 «Об обеспечении осуществления Министерством связи и массовых коммуникаций Российской Федерации функции головного удостоверяющего центра в отношении аккредитованных удостоверяющих центров»

На текущий момент используется технология односторонней кросс-сертификации

Аккредитация служб (TSP, OCSP и т.д.) удостоверяющих центров отсутствует

Система представления налоговой и бухгалтерской отчётности в электронном виде

Организатор – ФНС России

Способы представления:

1. Представление через Интернет-сайт ФНС России
2. Представление через специализированных операторов связи

Приказами ФНС России определены:

1. Организация и функционирование системы представления налоговых деклараций и бухгалтерской отчетности в электронном виде по телекоммуникационным каналам связи
2. Формы и форматы представления налоговых деклараций, бухгалтерской отчётности и иных документов
3. Унифицированный формат транспортного контейнера при информационном взаимодействии с приемными комплексами налоговых органов по телекоммуникационным каналам связи с использованием электронной цифровой подписи
4. Требования к криптографическим средствам

Количество участников системы - 75% налогоплательщиков из числа юридических лиц и индивидуальных предпринимателей

СПАСИБО ЗА ВНИМАНИЕ!

Вопросы?

Маслов Юрий

maslov@cryptopro.ru

+7 (495) 995-48-20

+7 (495) 984-07-90