*Санкт-Петербургский торгово-экономический институт*

**Кафедра информационных систем**
**и информационных технологий**

# Лекции по теме:
# «*Защита информации*»

***Версия от 12.02.2012***

http://egipko.narod.ru

*Подготовил доцент В.Н. Египко*

Санкт-Петербург
2012

*Тема лекции:*

# «Виды угроз и способы защиты информации»

# *Виды угроз для компьютерной информации:*

- потеря информации
- блокировка доступа к информации
- искажение или подмена информации
- несанкционированный доступ к информации и её копирование

# *Комплекс мер для защиты компьютерной информации:*

- организационные меры защиты информации
- аппаратные средства защиты информации
- программные средства защиты информации
- криптографическое обеспечение

# *Организационные меры защиты информации:*

Ограничение круга лиц, имеющих доступ к ресурсам вычислительных систем. Ограничения касаются использования принадлежащих пользователям сменных носителей (дискет, компакт-дисков и флэш-памяти), допуска на рабочие места посторонних лиц (детей или других родственников и знакомых сотрудников), а также самостоятельной установки или удаления программ.

# *Аппаратные средства защиты информации:*

- ***средства авторизации пользователей***: от считывателей магнитных карт до сканеров сетчатки глаза;
- источники бесперебойного питания (***ИБП,*** англ***., UPS – Uninterruptible Power Supply***);
- ***RAID-массивы***, обеспечивающие восстановление информации на диске и быструю замену неисправного диска без остановки работы системы (***«hot swap»***);
- ***кластеры*** из нескольких отдалённых компьютеров, совместно решающих общие задачи («горячее» резервирование).

# *Программные средства защиты информации:*

1. Ограничение бюджета (прав доступа) пользователей с применением логинов и паролей.
2. Резервное копирование (***backup***) при разработке документов.
3. Защита документов и архивов паролями двух типов .
4. Соблюдение пяти принципов долговременного хранения информации.
5. Использование антивирусных программ.
6. Использование брандмауэров (англ., ***firewall, файрволл)*** для защиты от несанкционированного доступа к компьютеру при подключении к *Internet.*
7. Шифрование данных, использование криптографических протоколов передачи (***SSL***, ***TLS***).
8. Сопровождение документов электронной цифровой подписью и сертификатом.
9. Ведение журналов протоколирования действий пользователей.

*Тема лекции:*

# «Электронная цифровая подпись»

# *Назначение ЭЦП*

1. **Контроль целостности** передаваемого документа: при любом случайном или преднамеренном изменении документа подпись станет недействительной, потому что вычислена она на основании исходного состояния документа и соответствует лишь ему.

2. **Защиту от изменений (подделки) документа**: гарантия выявления подделки при контроле целостности делает подделывание нецелесообразным в большинстве случаев.

3. **Невозможность отказа от авторства**. Так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, то владелец не может отказаться от своей подписи под документом.

4. **Доказательное подтверждение авторства документа**: Так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, то владелец пары ключей может доказать своё авторство подписи под документом. В зависимости от деталей определения документа могут быть подписаны такие поля, как «автор», «внесённые изменения», «метка времени» и т. д.

# *Примеры использования ЭЦП*:

1. Декларирование товаров и услуг (таможенные декларации)
2. Регистрация сделок по объектам недвижимости
3. Использование в банковских системах
4. Электронная торговля и госзаказы
5. Контроль исполнения государственного бюджета
6. В системах обращения к органам власти
7. Для обязательной отчетности перед государственными учреждениями
8. Организация юридически значимого электронного документооборота

# *Отечественные стандарты ЭЦП*

В 1994 году Главным управлением безопасности связи Федерального агентства правительственной связи и информации при Президенте Российской Федерации был разработан первый российский стандарт **ЭЦП** — ***ГОСТ Р 34.10-94.***

В 2002 году для обеспечения большей криптостойкости алгоритма взамен ГОСТ Р 34.10-94 был введен стандарт ***ГОСТ Р 34.10-2001***, основанный на вычислениях в группе точек эллиптической кривой. В соответствии с этим стандартом, термины «электронная цифровая подпись» и «цифровая подпись» являются синонимами.

Правовые условия использования **ЭЦП** в электронных документах регламентирует ***Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"***

# *Схемы построения ЭЦП:*

1. На основе алгоритмов *симметричного шифрования*. Данная схема предусматривает наличие в системе третьего лица — арбитра, пользующегося доверием обеих сторон. Авторизацией документа является сам факт шифрования его секретным ключом и передача его арбитру.
2. На основе алгоритмов *асимметричного шифрования*, в которых шифрование производится с помощью *открытого ключа*, а расшифровка — с помощью *закрытого* (*секретного*) ключа. В схеме же **ЭЦП** подписывание производится с применением *закрытого* ключа, а проверка — с применением *открытого* ключа. На данный момент такая схема построения **ЭЦП** наиболее распространена и находит широкое применение.

# *Этапы использования ЭЦП:*

1. **Генерация ключевой пары**. При помощи алгоритма генерации ключа равновероятным образом из набора возможных закрытых ключей выбирается *закрытый ключ* и вычисляется соответствующий ему *открытый ключ*.
2. **Формирование подписи**. Для заданного электронного документа с помощью *закрытого ключа* вычисляется **ЭЦП**.
3. **Проверка (верификация) подписи**. Для данных документа и подписи с помощью *открытого ключа* определяется действительность **ЭЦП**.

# *Управление и защита ключей ЭЦП:*

Задача защиты ключей от подмены решается с помощью *сертификатов*. В России юридически значимый сертификат ЭЦП выдаётся *удостоверяющими центрами,* имеющими соответствующие лицензии ФСБ РФ.

Особое внимание нужно уделять способу хранения закрытого ключа. Пользователь может хранить закрытый ключ на своем ПК, защитив его паролем. Однако такой способ хранения имеет ряд недостатков, в частности, защищенность ключа полностью зависит от защищенности компьютера, и пользователь может подписывать документы только на этом компьютере.

В настоящее время существуют следующие устройства хранения закрытого ключа: *смарт-карты, USB-брелоки и таблетки Touch-Memory*. Кража или потеря одного из таких устройств хранения может быть легко замечена пользователем, после чего соответствующий сертификат может быть немедленно отозван.

# *Устройства хранения закрытого ключа*


Смарт-карта и 5 видов USB-брелоков

# *Как получить ЭЦП?*

Процесс выдачи ЭЦП удостоверяющими центрами (УЦ) представляет собой проверку документов получателя ЭЦП (иначе говоря, идентификацию предполагаемого владельца ключа), генерацию пары ключей (открытого ключа, на который выпускается сертификат ЭЦП и который будет виден всем участникам документооборота, и закрытого ключа, известного только владельцу ЭЦП) и выпуск удостоверяющим центром сертификата открытого ключа в бумажном и электронном виде. Бумажный сертификат заверяется печатью УЦ и подписывается уполномоченным лицом УЦ, а электронный сертификат подписывается уполномоченным лицом УЦ с помощью собственной ЭЦП. После этого сертификат и ключевая пара записываются на ключевой носитель. В качестве ключевого носителя лучше всего использовать защищенные носители типа ruToken или eToken, представляющие собой флеш-устройства с интегрированными в них средствами обеспечения безопасности и конфиденциальности (требование ввода пин-кода, невозможность удаления или копирования ключевой пары).

# *Дополнительные условия работы с ЭЦП*

Для работы с ЭЦП необходимо установить на компьютер специальное программное обеспечение — *криптопровайдер*. Как правило, криптопровайдер можно приобрести в УЦ вместе с ЭЦП. Наиболее распространенными криптопровайдерами являются программы производства ООО «Лисси» (криптопровайдер «Lissi CSP») и ООО «Крипто-Про» (криптопровайдер «CryptoPro CSP»). После установки криптопровайдера необходимо вставить в компьютер ключевой носитель, после чего появляется возможность подписания документов.

С 01.01.2011 г. принимаются только ЭЦП, выданные авторизованными УЦ, т.е. УЦ, включенными в единое пространство доверия всех площадок и имеющими соответствующие соглашения.

При заказе ЭЦП следует сообщить сотруднику УЦ цель приобретения ключа, поскольку для придания подписанным документам юридической значимости соответствующая информация должна быть прописана УЦ в назначении сертификата.