1. Milanovic, B. Global income inequality by the numbers: In history and now / B. Milsnovic // Global Policy. – 2013. – Vol. 4., Issue 2. – P. 198–208.
2. Кудашова, Т. В. Влияние экономического роста и глобализации на неравенство по доходам населения в Республике Казахстан / Т. В. Кудашова // Вестник КазНУ. – 2012. – № 2 (90). – С. 23–27.
3. Воробьев, П. В. Влияние глобализации на экономическое неравенство стран мира :дис. … канд. экон. наук : 08.00.14 / П. В. Воробьев. – Екатеринбург, 2009. – 175 с.
4. Mills, M. Globalization and inequality / M. Mills // Europ. sociological rev. – 2009. – Vol. 25, № 1. – P. 1–8
5. Maskin, E. Why Haven't Global Markets Reduced Inequality in Emerging Economies? / E. Maskin // The world bank economic review. – 2015. – Vol. 29. – P. 48–52.
6. Dollar, D. Spreading the wealth / D. Dollar, A. Kraay // Foreign affairs. –2002. – Vol. 81. – P. 120–133.

Программно-аппаратная защита информации от локальногонесанкционированного доступа

Ковалькова И.А.
Белорусский национальный технический университет

Современная информационная компьютерная система представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя.

Информационная безопасность –это основа всей системы безопасности компьютерных систем. Именно она позволяет обеспечивать конфиденциальность, целостность и доступность информации. Информационная безопасность характеризуется отсутствием недопустимого риска, связанного с утечкой информации вследствие несанкционированного доступа(НСД).

Несмотря на то, что современные ОС для персональных компьютеров имеют собственные подсистемы защиты, актуальность создания дополнительных средств защиты

сохраняется. Большинство компьютерных систем не способны защитить данные, находящиеся за их пределами. И в этих случаях для защиты данных используются ***аппаратно-программные средства*** защиты информации.

Применение так называемой двухфакторной аутентификации, при которой пользователь для входа в систему должен не только ввести *пароль*, но и предъявить *элемент аппаратного обеспечения*, содержащий подтверждающую его подлинность ключевую информацию, даёт дополнительную защиту информации от НСД.

Такими элементами аппаратного обеспечения могут быть:

- *магнитные диски*, не требующие установки на компьютере пользователя КС никаких дополнительных аппаратных средств, но наиболее уязвимые с точки зрения копирования хранящейся на них информации;
- *элементы TouchMemory*, включающие в себя энергозависимую память в виде постоянного запоминающего устройства (ПЗУ) с уникальным для каждого изделия серийным номером и оперативного запоминающего устройства (ОЗУ) для хранения идентифицирующей пользователя информации, а также встроенный элемент питания со сроком службы до 10 лет (элемент TouchMemory напоминает миниатюрную батарейку диаметром 16 мм и толщиной 3-6 мм, он имеет один сигнальный контакт и один контакт заземления, а для контакта элемента с устройством чтения достаточно простого касания);
- *пластиковые карты с магнитной полосой*, на которой помимо ключевой информации могут размещаться и дополнительные реквизиты пользователя – его фамилия, имя, отчество, фотография, название организации и т.п. (подобные карты наиболее дешёвы, но и наименее защищены от копирования и подделки);
- *карты со штрихкодом*, покрытым непрозрачным составом, считывание информации с которых происходит в инфракрасных лучах (эти карты относительно дешёвы, но уязвимы для подделки);
- *смарт-карты*, носителем ключевой информации в которых является специальная бескорпусная микросхема, включающая в себя только память для хранения ключевой информации (простые смарт-карты) или микропроцессор

(интеллектуальные карты), позволяющие реализовывать достаточно сложные процедуры аутентификации;

- *маркеры eToken* (*USB-брелки*), представляющие собой подключаемое к USB-порту компьютера устройство, которое включает в себя аналогичную смарт-карте микросхему с процессором и защищённой от несанкционированного доступа памятью (в отличие от пластиковых карт не требует установки устройства их чтения с кабелем для подключения этого устройства

к компьютеру).

Рис. 1.Смарт-картаи USB-ключ eToken PRO, eToken NG-FLASH, eToken NG-OTP, eToken PRO (Java) и eToken PASS.

Программные средства системы защиты информации должны быть записаны на плате расширения BIOS, для каждой из которых определён уникальный пароль установки. Установка системы защиты информации производится на компьютере, свободном от вредоносных программ типа закладок и вирусов.

После установки платы расширения BIOS выполняется процедура установки системы защиты информации:

1) после включения питания компьютера программа, записанная на плате расширения BIOS, выдаёт запрос на ввод пароля;

2) после ввода пароля установки (как правило, администратором системы) происходит загрузка операционной

системы и запуск программы установки (проверочные функции системы защиты при этом отключаются);

3) по запросу программы установки вводятся пароль пользователя, ключевая информация с элемента аппаратного обеспечения (например, серийный номер элемента TouchMemory) и имена подлежащих проверке системных и пользовательских файлов;

4) для каждого указанного файла вычисляется и сохраняется проверочная информация.

Процедура входа пользователя в КС при использовании программно-аппаратной системы защиты от НСД, следующая:

1) после включения питания компьютера программа на плате расширения BIOS запрашивает пароль пользователя и просит установить элемент аппаратного обеспечения с его ключевой информацией;

2) осуществляется проверка целостности выбранных при установке системы защиты файлов;

3) в зависимости от результатов проверки выполняется либо загрузка операционной системы, либо запрос на повторный ввод пароля.

После завершения работы пользователя элемент аппаратного обеспечения с его ключевой информацией изымается из компьютера.