Организация защиты информации в персональных компьютерах

Домбровская Л. А.[1], Яковлева Н. А.[2], Васютина Т. Л.[3]

Домбровская Лариса Александровна / Dombrovskaya Larisa Alexandrovna – кандидат педагогических наук, доцент;
Яковлева Наталья Александровна / Yakovleva Natalia Alexandrovna - кандидат психологических наук;
Васютина Татьяна Львовна /Vasyutina Tatiana Lvovna – кандидат технических наук, доцент,
кафедра математики и информатики,
Санкт-Петербургский университет МВД России, г. Санкт-Петербург

Аннотация: *в статье рассмотрены вопросы защиты информации в персональных компьютерах. Причины активизации компьютерных преступлений. Формирование множества возможных подходов к защите информации в ПК.*

Ключевые слова: *информационная безопасность, установка паролей, определение подлинности электронной подписи, обеспечение конфиденциальности информации.*

В настоящее время никто не будет спорить о пользе и необходимости использования персональных компьютеров в любой сфере человеческой деятельности. Массовое распространение ПК привело к резкому повышению интенсивности циркуляции информации, децентрализации процессов ее хранения и обработки, существенного изменения структуры и содержания информационных технологий.

Однако, безусловно, важнейшее изобретение компьютера и дальнейшее бурное развитие информационных технологий во второй половине XX века сделали проблему защиты информации настолько актуальной и острой, насколько актуальна сегодня информатизация для всего общества. И одной из тенденций, характеризующих развитие современных информационных технологий, является рост числа компьютерных преступлений и связанных с ними хищений конфиденциальной и иной информации, а также материальных потерь.

Причин активизации компьютерных преступлений и связанных с ними финансовых потерь как государственных и коммерческих организаций разного уровня, так и отдельных пользователей достаточно много, существенными из них являются:

- переход от традиционной «бумажной» технологии хранения и передачи сведений на электронную и недостаточное при этом развитие технологии защиты информации в таких технологиях;
- объединение вычислительных систем, создание глобальных сетей и расширение доступа к информационным ресурсам;
- увеличение сложности программных средств и связанное с этим уменьшение их надежности и увеличением уязвимостей и другие.

Стандартность аархитектурных принципов построения, оборудования и программного обеспечения персональных компьютеров, высокая мобильность программного обеспечения и ряд других признаков определяют сравнительно легкий доступ профессионала к информации, находящейся в ПК. Если персональным компьютером пользуется группа пользователей, то может возникнуть необходимость в ограничении доступа к информации различных потребителей.

В этих условиях заботу о защите информации на личном ПК должны проявлять сами пользователи, которые не только не являются профессионалами в области защиты, но нередко вообще имеют лишь навыки непосредственного решения ограниченного набора задач. Этими особенностями и обусловлена необходимость самостоятельного рассмотрения вопросов защиты информации в персональных ЭВМ с акцентированием внимания именно на внутренней защите.

На формирование множества возможных подходов к защите информации в ПК и выбор наиболее целесообразного из них в конкретных ситуациях определяющее влияние оказывают следующие факторы [4, 5, 6]:

1) цели защиты;
2) потенциально возможные способы защиты;
3) имеющиеся средства защиты.

Основные цели защиты информации:

– обеспечение физической целостности;
– обеспечение логической целостности;
– предупреждение несанкционированного получения;
– предупреждение несанкционированной модификации;
– предупреждение несанкционированного копирования.

Обеспечение логической целостности информации для ПК мало актуально, другие же цели применительно к ПК можно было конкретизировать следующим образом.

Обеспечение физической целостности [2].

Физическая целостность информации в ПК зависит от целостности самого ПК, целостности дисков и дискет, целостности информации на дисках, дискетах и в оперативной памяти. В широком спектре угроз целостности информации в ПК следует обратить особое внимание на угрозы, связанные с недостаточно высокой квалификацией большого числа владельцев ПК. В этом плане особо опасной представляется возможность уничтожения или искажения данных на жёстком диске (винчестере), на котором могут накапливаться очень большие объёмы данных самим пользователем.

Предупреждение несанкционированной модификации.

Довольно опасной разновидностью несанкционированной модификации информации в ПК является действие вредоносных программ (компьютерных вирусов), которые могут разрушать или уничтожать программы или массивы данных. Данная опасность приобретает актуальность в связи с тем, что среди владельцев ПК общепринятой становится практика обмена носителями информации, среди которых в настоящее время получили флэш-носители.

Предупреждение несанкционированного получения информации, находящейся в ПК.

Данная цель защиты приобретает особую актуальность в тех случаях, когда хранимая или обрабатываемая информация содержит тайну того или иного характера (государственную, коммерческую и т. п.). Возможности несанкционированного получения информации в современных ПК очень широки и разнообразны, поэтому данный вид защиты требует серьёзного внимания.

Предупреждение несанкционированного копирования информации.

Актуальность данной разновидности защиты определяется следующими тремя обстоятельствами [1, 3]:

– накопленные массивы информации все больше становятся товаром;

– все более широкое распространение получает торговля компьютерными программами;

– оптические дисководы с перезаписью, флеш-носители создают весьма благоприятные условия для широкомасштабного копирования информации ПК.

Применительно к защите информации в ПК, учитывая особенности архитектурного построения и способов использования ПК, можно выделить ряд угроз (каналов) утечки информации.

Характерные для ПК каналы принято классифицировать по типу средств, которые используются в целях несанкционированного получения по ним информации, причем выделяются три типа средств: человек, аппаратура, программа.

Группу каналов, в которых основным средством несанкционированного получения информации является человек, составляют:

– хищение носителей информации (магнитных, CD-дисков, распечаток и т. д.);

– чтение или фотографирование информации с экрана;

– чтение или фотографирование информации с распечаток.

В группе каналов, основным средством использования которых служит аппаратура, выделяют:

– подключение к устройствам ПК специальной аппаратуры, с помощью которой можно уничтожать или регистрировать защищаемую информацию;

– регистрацию с помощью специальных средств электромагнитных излучений устройств ПК в процессе обработки защищаемой информации.

Третью группу каналов (основное средство использования которых – программы) образуют:

– программный несанкционированный доступ к информации;

– уничтожение (искажение) или регистрация защищаемой информации с помощью программных закладок или ловушек;

– чтение остаточной информации из ОЗУ;

– программное копирование информации с магнитных носителей.

Учитывая, что ПК работают не только автономно, но и имеют выход в сеть – локальную или глобальную, то появляются каналы сопряжения соответствующего вида.

Тогда полный базовый перечень тех участков (мест), в которых могут находиться защищаемые данные, может быть представлен в следующем виде: системные платы ПК; современные накопители; ВЗУ типа «Винчестер»; дисплей; печатающее устройство; каналы сопряжения. Защите подлежат данные, находящиеся в каждом из перечисленных мест.

В соответствии с изложенным каждый пользователь ПК может применительно к своим условиям составить перечень потенциально возможных угроз его информации и на этой основе целенаправленно решать вопросы надёжной ее защиты. При этом следует иметь в виду существующие современные методы и средства защиты информационных систем:

организационно-технические;

административно-правовые;

программно-технические.

Применительно к защите индивидуальных ПК для пользователя наиболее целесообразно применение, в первую очередь, программно-технических мер защиты.

Программно-технические средства предназначены для предотвращения нарушения конфиденциальности и целостности данных, хранимых и обрабатываемых в информационной системе (в частности в ПК). Нарушение целостности – это несанкционированное внесение изменений в данные.

Рассмотрим наиболее важные для пользователя меры защиты информации в своём ПК.

Обеспечение целостности информации в ПК.

Следует отметить, что угрозы целостности информации в ПК, как и в любой другой автоматизированной системе, могут быть случайными и преднамеренными. Основными разновидностями случайных угроз являются отказы, сбои, ошибки, стихийные бедствия и побочные явления, а конкретными источниками их проявления — технические средства, программы и пользователи. С учётом современного состояния технических и программных средств ПК, а также способов и средств их использования к наиболее реальным угрозам целостности информации случайного характера следует отнести ошибки пользователей. Основными из этих ошибок являются неправильные обращения к серийным компонентам программного обеспечения.

Более серьёзную опасность целостности информации в ПК представляют преднамеренные угрозы, создаваемые людьми в злоумышленных целях. Такая угроза может быть непосредственной, если злоумышленник получает доступ к ПК, и опосредованной, когда угроза создаётся с помощью промежуточного носителя. Из преднамеренных угроз наибольшее распространение получили так называемые разрушающие программные средства (РПС): электронные вирусы, черви, троянские кони и др. Они же представляют и наибольшую опасность целостности информации в ПК.

Действенным методом сохранения целостности информации в ПК является в частности ее резервное копирование.

Защита ПК от несанкционированного доступа.

Для сохранения конфиденциальности своей информации пользователь должен особенно позаботиться об оснащении используемой ПК высокоэффективными средствами защиты от НСД.

Основные механизмы защиты ПК от НСД могут быть представлены следующим перечнем:

1) физическая защита ПК и носителей информации;

2) опознавание (аутентификация) пользователей и используемых компонентов обработки информации;

3) разграничение доступа к элементам защищаемой информации;

4) криптографическое закрытие защищаемой информации, хранимой на носителях (архивация данных);

5) криптографическое закрытие защищаемой информации в процессе непосредственной ее обработки;

6) регистрация всех обращений к защищаемой информации.

В настоящее время в арсенале пользователя имеется достаточно большое количество конкретных способов защиты информации в ПК.

Перечислим с краткими пояснениями наиболее популярные и доступные из них.

Установка паролей на начальную загрузку ПК. Для защиты ПК BIOS поддерживает установку двух типов паролей:

User Password – пароль на возможность начальной загрузки ПК, запрашивается после тестирования аппаратного обеспечения и собственно перед загрузкой любой ОС;

Supervisor Password – пароль полного доступа к BIOS, он же пароль администратора BIOS, включает в себя возможность изменения настроек BIOS и возможность начальной загрузки ПК.

Данный способ позволяет запретить загрузки операционной системы без пароля, тем самым обеспечивается относительная защита данных даже на FAT-разделах, а также дополнительная аутентификация пользователей не зависимо от средств самой ОС, установленной на ПК.

Шифрование защищаемой информации (криптография) – обеспечивается защита данных при хранении/передаче/транспортировке информации.

Невосстановимое удаление данных – навсегда стереть секретные данные с носителей информации. Например, с помощью программного обеспечения Acronis Drive Cleanser 6.0.

По WWW без следов. Цель данного способа – сокрытие посещённых веб-страниц, а также личных данных при посещении Интернета.

Примерная методика: открыть «Пуск - Панель управления - Свойства обозревателя». В появившемся диалоге нажать кнопки <Удалить «Cookie»> и <Удалить файлы>. В результате будут удалены все файлы из папки временных файлов Интернета, а также файлы Cookie. Отключить сохранение временных файлов можно, нажав на кнопку <Параметры…> и установив флаг «Никогда», а также задав размер занимаемого места на диске равным 0.

Также следует уничтожить все компрометирующие посещения Интернета из журнала посещённых страниц: открыть Internet Explorer. Меню «Вид - Панели обозревателя - Журнал». Затем в появившемся окне выбрать и удалить нужные записи из журнала. Они разбиты по дням и страничкам.

Отключение автозапуска Flash - накопителей/CD

В Интернете предлагается несколько вариантов методики такого отключения. Один из них:

Пуск - Выполнить - gpedit.msc

Конфигурация компьютера

Административные шаблоны

Система

Отключить автозапуск

Правой кнопкой мыши - Свойства - Включена - Всех дисководах - Применить.

После этого автозагрузка на флажках не стартует и вирусы не смогут распространиться без помощи пользователя.

Защита Flash-накопителей от вирусов. Цель – не позволить проникнуть вирусам в корневой каталог флешки. Однако известно, что тип файловой системы флешки по умолчанию FAT 32, но в этой системе запрет доступа не выставляется. Для того чтобы это реализовать, нужно сменить файловую систему флешки на NTFS, это возможно даже без удаления данных с флеши. В Интернете приводится наглядная инструкция, как ограничить доступ в корень флешки.

Прием и анализ почты. Использование почтовых программ, которые транслируют исходные тексты из HTML в простои текст. Потому что именно в HTML и вставляются апплетики на JAVA, которые могут привести к изменению интерфейса. Кроме того, для защиты от сетевых червей помогут почтовые платины[1] от известных антивирусных пактов, которые сканируют ПК на вирусы.

Использование брандмауэра. Цель – защита ПК от несанкционированного доступа со стороны других компьютеров локальной сети или сети Интернет.

В персональном брандмауэре устанавливаются параметры, регулирующие функционирование ПК в сети, например:

какие программы имеют право на выход в сеть;

правила пропуска пакетов из сети;

список доверенных сетевых адресов.

В операционную систему Windows, начиная с XP, встроен персональный брандмауэр, выполняющий вышеперечисленные функции. Будучи включенным, брандмауэр блокирует доступ к компьютеру из сети.

В заключение следует отметить, что в небольшом обзоре способов защиты информации в ПК пользователем невозможно охватить весь спектр вопросов и ответов на них в этой области, найденных на сегодняшний день. Проблем обеспечения безопасности информации в ПК еще очень много. Но риск можно свести к минимуму, используя комплексные подходы, которые были рассмотрены выше.

Литература

1. *Парфенов Н. П., Стахно Р. Е.* Технология защиты персональных данных // Наука, техника и образование, 2016. № 4.
2. *Стахно Р. Е., Гончар А. А.* Защита информации в современном документообороте // Наука, техника и образование, 2016. № 4.
3. *Домбровская Л. А., Яковлева Н. А., Стахно Р. Е.* Современные подходы к защите информации, методы, средства и инструменты защиты // Наука, техника и образование, 2016. № 4.
4. Сайт Безопасник. [Электронный ресурс]. Режим доступа: http://www.bezopasnik.org2 (дата обращения: 27.10.2016).
5. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». [Электронный ресурс]. Режим доступа: http://www.consultant.ru (дата обращения: 27.10.2016). .
6. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных" (с изм. и доп., вступ. в силу с 01.09.2015). [Электронный ресурс]. Режим доступа: http://www.consultant.ru (дата обращения: 27.10.2016).

[1] Независимо компилируемый программный модуль, динамически подключаемый к основной программе и предназначенный для расширения и/или использования её возможностей.