Безопасность информации

Информационная безопасность

Включает в себя следующие понятия

- Конфиденциальность: обеспечение доступа к информации только авторизованным пользователям.
- Целостность: обеспечение достоверности и полноты информации и методов её обработки.
- Доступность: обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Группы на которые делятся средства защиты информации

- законодательные (международные конвенции, конституционные нормы, федеральные законы и акты,)
- физические (средства физического ограничения доступа к информации: ограждения, сейфы и т.д.)
- аппаратные (технические)
- программные
- криптографические

Законодательные средства защиты

Базовым в этом отношении является Закон Российской Федерации "Об информации, информатизации и защите информации", принятый 25 января 1995 г. В соответствии с ним любой российский гражданин может предпринимать необходимые меры для предотвращения утечки, хищения, утраты, искажения и подделки информации. Вопрос состоит в том, какие действия являются на самом деле необходимыми для адекватной защиты вашей информации.

Законодательные средства защиты

- Главной вехой в цепочке этих изменений стало введение в действие 1 января 1997г. нового Уголовного кодекса. В нем содержится глава "Преступления в сфере компьютерной информации", где перечислены следующие преступления:

Законодательные средства защиты

- **неправомерный доступ к компьютерной информации (статья 272):**
- **создание, использование и распространение вредоносных компьютерных программ (статья 273);**
- **нарушение правил эксплуатации компьютеров, компьютерных систем и сетей (статья 274).**

Отметим, что уголовная ответственность за перечисленное наступает только в том случае, когда уничтожена, блокирована, модифицирована пли скопирована информация, хранящаяся в электронном виде.

Безопасность информации на компьютере

- **В процессе эксплуатации компьютера по самым разным причинам возможны** (и часто происходят) **порча и потеря информации**, находящейся на жестких дисках компьютера.

Основные причины потери информации на компьютере (пронумерованы по значимости)

1. **ошибочными действиями пользователей**, (чаще всего)
2. некорректной работой программ
3. сбоями в электропитании
4. авариями жестких дисков
5. компьютерными вирусами,
6. Несанкционированными действиями третьих лиц и т.д.

Классификация информации по срочности хранения и важности самой информации

- Краткосрочная информация – информация, которая подлежит обновлению (копированию) от нескольких раз в день, до одного раза в месяц
- Средне срочная информация – информация, которая обновляется от одного раза в месяц до одного раза в год
- Долгосрочная информация, которая обновляется от одного раза в год, до постоянного хранения.

Соответственно по важности информацию можно поделить так же на три группы:

- Информация низкой степени важности, которая может быть либо восстановлена из каких либо источников, либо получена заново
- Информация средней степени важности, которая в принципе может быть утеряна без восстановления, однако не является очень ценной
- Информация высокой степени важности, которая не подлежит восстановлению и потеря которой является существенной проблемой для пользователя.

- ***Резервирование данных***

Единственный надежный способ предотвращения потери информации и соответствующих (иногда очень существенных) потерь времени и денег — это создание ***резервных копий*** данных, то есть копий, позволяющих восстановить данные при их повреждении или утрате.

Процесс создания резервных копий обычно называется *резервированием*.

Автоматическое резервирование.

Устройства для хранения данных

- 1. Винчестеры
- 2. Оптические диски
- 3. Электронные носители
- 4. Облачные хранилища.

- Справочная информация о сроках хранения данных на различных типах носителей:
- 1. Оптические диски : CD, DVD и Blu Ray. Могут хранить информацию от 2-3 лет до 50. В каждом конкретном случае срок хранения зависит от качества оптического диска и от условий хранения. Наибольший вред оптическим устройствам памяти наносят: механические повреждения, прямой солнечный свет и замутнение защитного слоя.
- 2. НДД накопители – «винчестеры». Могут хранить информацию от 2-3 до 10 лет. Наибольший вред «винчестерам» наносят электромагнитные излучения, механические повреждения нарушения температурного режима хранения и влажности – что приводит к высыханию магнитного слоя и его обсыпанию.
- 3. Электронная память: USB флэш накопители, карты памяти и пр. Могут хранить информацию от 2-3 месяцев до 10 лет. Мало чувствительны к внешним воздействиям, исключая экстремальные воздействия. Основные причины выхода из строя связаны с поломками электроники. Рекомендуется покупать для хранения устройства долговременной памяти известных производителей (брендов).

Облачные хранилища

- 3. С развитием Интернет все более популярным становится хранение информации на сетевых серверах. Создаются даже специальные облачные хранилища информации.
- Такая информация имеет очень низкую защиту от доступа к ней не авторизованных пользователей (если у этих пользователей все-таки возникает желание получить доступ к этой информации) и то, что доступ к такой информации полностью зависит от владельца такого сервера, который по своему желанию может отключить его в любой момент.
- Заботу о целостности информации несет непосредственно хостинг-провайдер у которого расположена эта информация и целостность такой информации может быть гораздо выше, чем целостность обеспечиваемая самим пользователем.

Ценность информации

Наибольшую ценность представляет авторская информация:

- Домашнее фото и видео и аудио записи
- Письма, документы, статьи и т.д.
- Наиболее ценную информацию рекомендуется хранить вне компьютера.
- На компьютере информацию лучше хранить на отдельном несистемном диске

Ограничение доступа

Для обеспечения безопасности данных очень полезно применение простых, но эффективных мер по ограничению доступа к этим данным:

Установление паролей:

- **На BIOS** – ограничивает доступ к аппаратным устройствам компьютера;
- **На загрузку ОС или конкретного пользователя** – не позволяет запускать компьютер со стандартной ОС;
- **На устройства и элементы данной ОС** (диски, принтеры, папки, файлы, программы и т.д.)
- **На редактирование реестра и другие элементы настройки ОС.**

Аппаратная защита

- Аппаратные ключи
- Источники бесперебойного питания
- Дублирование устройств компьютера
- Резервные серверы (дублирование самих компьютеров)

Шифрование

Используется для хранение и передаче конфиденциальных и секретных данных

- Если на компьютере, к которому может иметь доступ более одного человека, необходимо держать конфиденциальные данные, их следует хранить в зашифрованной форме — скажем, в защищенном паролем архиве программ PKZIP или ARJ или на защищенном паролем диске (NDisk),
- Следует помнить, что все стандартные способы шифрования данных ненадежны против серьезного взлома — существуют даже программы, взламывающие пароли, и эти программы легко доступны.
- Для действительно секретных данных или данных, представляющих серьезный коммерческий интерес, такие методы не годятся. Для этих целей необходимо использовать специальные средства, либо средства, изготовленные самостоятельно.

Защита от компьютерных вирусов

- **Компьютерные вирусы — это специально написанные программы, которые могут записывать** (внедрять) **свои копии** (возможно, измененные) **в компьютерные программы**, расположенные в исполнимых файлах, системных областях дисков, драйверах, документах и т.д., причем эти копии сохраняют возможность к «размножению».
- Программа или иной объект, содержащие вирус, называются *зараженными.* Зараженными могут быть исполнимые файлы, программы начальной загрузки жесткого диска или дискеты, файлы драйверов, командные файлы DOS, документы Word для Windows, электронные таблицы в формате Excel и т.д.

Антивирусные программы

- **Антивирусная программа** (**антивирус**) — изначально программа для обнаружения и лечения (восстановления) от вредоносных объектов инфицированных файлов, а также для профилактики — предотвращения заражения файла или операционной системы вредоносным кодом.

Антивирусные программы

- Многие современные антивирусы позволяют обнаруживать и удалять также троянские программы и прочие вредоносные программы. Так же существуют программы - файрволы, которые также способствуют защите компьютерных сетей или отдельных узлов от несанкционированного доступа, однако их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации, т.е. от несанкционированного доступа извне или, наоборот, для ограничения связи программ с внешними источниками из-за возможной утечки информации.

Антивирусные программы

- Антивирусное программное обеспечение состоит из подпрограмм, которые пытаются обнаружить, предотвратить размножение и удалить компьютерные вирусы и другие вредоносные программы, но ни одна из них не даст 100% защиты.

Антивирусные программы

- Основные принципы заложенные в антивирусных программах :
- Вирусные базы – уже найденные и определённые кем-то программы, как вирусные, заносятся и хранятся в таких базах. Их нужно периодически обновлять.
- Аналитическое (эвристическое) определение вирусных программ по нестандартным, несанкционированным действиям.
- Антивирусные программы могут допускать ошибки.

Защита информации на персональном компьютере (ПК).

- Основными способами защиты информации на ПК является:
- Установка паролей на BIOS и на вход пользователя в операционную систему.
- Установка блоков бесперебойного питания на сетевое питающее напряжение (UPS)
- Резервирование данных при работе пользователя.
- Важно понимать, что любая информация хранящаяся на ПК может быть найдена и прочитана. Это вопрос времени и денег.

Защита информации в локальных проводных сетях.

- Основными способами защиты информации в локальных сетях является:
- Администрирование – установления различного приоритета (прав) различным пользователям на доступ к управлению информацией и её редактированием (изменением).
- Подтверждение прав пользователя (идентификация и паролирование) при выполнении наиболее важных операций с информацией.

Защита информации в беспроводных сетях.

- Основными способами защиты информации в беспроводных сетях является:
- Идентификация пользователей и устройств в беспроводной сети при подключении.
- Шифрование информации передаваемой по беспроводной сети.

Защита информации в сети интернет (глобальных сетях).

- Основными способами защиты информации в интернет является:
- Идентификация пользователей и устройств сети при подключении к различным сайтам.
- Шифрование информации передаваемой по сетям интернет.
- Важно понимать, что защитить информацию, расположенную в сети интернет от скачивания (копирования) невозможно. Можно только затруднить этот процесс.

Защита информации в социальных сетях.

- Использование социальных сетей для общения и передачи информации для определенного круга лиц в настоящее время приводит к тому, что получение доступа к чужим личным страничкам в социальных сетях является становится весьма частым способом несанкционированного использования информации.
- Установка сложного пароля на вход на свою личную страничку. Лучше всего, если пароль будет содержать не менее 8 символов, включая символы верхнего и нижнего регистров, цифры и символы, не являющиеся ни буквами и не цифрами.
- Не размещать в социальных сетях важную конфиденциальную информацию, получение несанкционированного доступа к которой может нанести вред пользователю.

- Ни в коем случае нельзя давать пароли, связанные с именами (родственников, детей, и пр.), прозвищами, кличками домашних питомцев, связанных с датой рождения (своей или близких), а так же часто используемых слов при обращении (киска, зайчик, рыбка и пр.). Такие пароли довольно легко подбираются.
- Чаще всего взлом личных страничек выполняется не подбором пароля, а просто кражей этого пароля. Поэтому очень важно следить за тем, что бы пароли не попадали к другим пользователям, даже близким.

- Следует периодически менять пароли (от 1 раза в месяц, до 1 раза в год) на важные объекты в вычислительной технике и компьютерных сетях.
- Большой проблемой при работе с социальными сетями является потеря логина и пароля самим пользователем и, в следствие этого, потеря информации, которая хранится на социальной страничке. Это связано с тем, что рядовой пользователь устанавливает автоматический ввод логина и пароля на вход в свою страничку из своего браузера. Поэтому, рекомендуется все пароли и логины записывать и хранить вне компьютера, лучше всего на бумажном носителе
- Важно понимать, что информация, размещенная в социальных сетях с большой вероятностью может быть утеряна или похищена и, ни в коем случае не размещать там информацию, представляющую большую ценность.