Обучающиеся группы № 30
Приветствую вас на дистанционном обучении

Работы прошу высылать на адрес
msn@apt29.ru (Мамонов Сергей Николаевич)

Задание:

1. Внимательно изучить теоретические сведения к практическому занятию.

2. В тетради, письменно, выполнить контрольные задания.

3. Результат работы прислать для проверки на электронный адрес: msn@apt29.ru

Практическое занятие
Тема: Правовые нормы в информационной деятельности

Цель: Изучить правовые нормы в информационной деятельности человека.

Теоритические сведения к практической работе

Правовое регулирование

Принимая во внимание, что информация практически ничем не отличается от другого объекта собственности, например машины, дома, мебели и прочих материальных продуктов, следует говорить о наличии подобных же прав собственности и на информационные продукты. Право собственности состоит из трех важных компонентов: права распоряжения, права владения и права пользования.

- ♦ Право распоряжения состоит в том, что только субъект-владелец информации имеет право определять, кому эта информация может быть предоставлена.
- ♦ Право владения должно обеспечивать субъекту-владельцу информации хранение информации в неизменном виде. Никто, кроме него, не может ее изменять.
- ♦ Право пользования предоставляет субъекту-владельцу информации право ее использования только в своих интересах.

Таким образом, любой субъект-пользователь обязан приобрести эти права, прежде чем воспользоваться интересующим его информационным продуктом. Это право должно регулироваться и охраняться государственной инфраструктурой и соответствующими законами. Как и для любого объекта собственности, такая инфраструктура состоит из цепочки:

законодательная власть (законы) -> судебная власть (суд) -> —» исполнительная власть (наказание).

Любой закон о праве собственности должен регулировать отношения между субъектом-владельцем и субъектом-пользователем. Такие законы должны защищать как права собственника, так и права законных владельцев, которые приобрели информационный продукт законным путем. Защита информационной собственности проявляется в том, что имеется правовой механизм защиты информации от разглашения, утечки, несанкционированного доступа и обработки, в частности копирования, модификации и уничтожения.

В Российской Федерации принят ряд указов, постановлений, законов, таких как: «Об информации, информатизации и защите информации», «Об авторском праве и смежных

правах», «О правовой охране программ для ЭВМ и баз данных», «О правовой охране топологий интегральных схем» и т. д.

Закон Российской Федерации «Об информации, информатизации и защите информации» является базовым юридическим документом, открывающим путь к принятию дополнительных нормативных законодательных актов для успешного развития информационного общества. С его помощью частично удается решить вопросы правового урегулирования ряда проблем: защиты прав и свобод личности от угроз и ущерба, связанных с искажением, порчей и уничтожением «персональной» информации.

Закон состоит из 25 статей, сгруппированных по пяти главам:

- ❖ общие положения;
- ❖ информационные ресурсы;
- ❖ пользование информационными ресурсами;
- ❖ информатизация, информационные системы, технологии и средства их обеспечения;
- ❖ защита информации и прав субъектов в области информационных процессов и информатизации.

Закон создает условия для включения России в международный информационный обмен, предотвращает бесхозяйственное отношение к информационным ресурсам и информатизации, обеспечивает информационную безопасность и права юридических и физических лиц на информацию. В нем определяется комплексное решение проблемы организации информационных ресурсов, определяются правовые положения по их использованию. Информационные ресурсы предлагается рассматривать в двух аспектах:

- ♦ как материальный продукт, который можно покупать и продавать;
- ♦ как интеллектуальный продукт, на который распространяются право интеллектуальной собственности и авторское право.

Чрезвычайно важно и актуально принятие таких правовых актов, которые смогли бы обеспечить:

- охрану прав производителей и потребителей информационных продуктов и услуг;
- защиту населения от вредного влияния отдельных видов информационных продуктов;
- правовую основу функционирования и применения информационных систем, Интернета, телекоммуникационных технологий.

Информационная безопасность для различных пользователей компьютерных систем

Определим несколько видов деятельности, например:

- решение прикладных задач, где отражается специфика деятельности конкретного пользователя-специалиста;
- решение управленческих задач, что характерно для любой компании;
- оказание информационных услуг в специализированной компании, например информационном центре, библиотеке и т. п.;
- коммерческая деятельность;
- банковская деятельность.

Методы защиты информации

При разработке методов защиты информации в информационной среде следует учесть следующие важные факторы и условия:

- ➢ расширение областей использования компьютеров и увеличение темпа роста компьютерного парка (то есть проблема защиты информации должна решаться на уровне технических средств);

- высокая степень концентрации информации в центрах ее обработки и, как следствие, появление централизованных баз данных, предназначенных для коллективного пользования;
- расширение доступа пользователя к мировым информационным ресурсам (современные системы обработки данных могут обслуживать неограниченное число абонентов, удаленных на сотни и тысячи километров);
- усложнение программного обеспечения вычислительного процесса на компьютере, так как современные компьютеры могут работать:
  - в мультипрограммном режиме, когда одновременно решается несколько задач;
  - в мультипроцессорном режиме, когда одна задача решается несколькими параллельно работающими процессорами;
  - в режиме разделения времени, когда один и тот же компьютер может одновременно обслуживать большое количество абонентов.

К традиционным методам защиты от преднамеренных информационных угроз относятся: ограничение доступа к информации, шифрование (криптография) информации, контроль доступа к аппаратуре, законодательные меры. Рассмотрим эти методы.

Ограничение доступа к информации осуществляется на двух уровнях:

- на уровне среды обитания человека, то есть путем создания искусственной преграды вокруг объекта защиты: выдачи допущенным лицам специальных пропусков, установки охранной сигнализации или системы видеонаблюдения;
- на уровне защиты компьютерных систем, например, с помощью разделения информации, циркулирующей в компьютерной системе, на части и организации доступа к ней лиц в соответствии с их функциональными обязанностями. При защите на программном уровне каждый пользователь имеет пароль, позволяющий ему иметь доступ только к той информации, к которой он допущен.

Шифрование (криптография) информации заключается в преобразовании (кодировании) слов, букв, слогов, цифр с помощью специальных алгоритмов. Для ознакомления с шифрованной информацией нужен обратный процесс — декодирование. Шифрование обеспечивает существенное повышение безопасности передачи данных в сети, а также данных, хранящихся на удаленных устройствах.

Контроль доступа к аппаратуре означает, что вся аппаратура закрыта и в местах доступа к ней установлены датчики, которые срабатывают при вскрытии аппаратуры. Подобные меры позволяют избежать, например, подключения посторонних устройств, изменения режимов работы компьютерной системы, загрузки посторонних программ и т. п.

Законодательные меры заключаются в исполнении существующих в стране законов, постановлений, инструкций, регулирующих юридическую ответственность должностных лиц — пользователей и обслуживающего персонала за утечку, потерю или модификацию доверенной им информации.

При выборе методов защиты информации для конкретной компьютерной сети необходим тщательный анализ всех возможных способов несанкционированного доступа к информации. По результатам анализа проводится планирование мер, обеспечивающих необходимую защиту, то есть осуществляется разработка политики безопасности.

***Политика безопасности* — это совокупность технических, программных и организационных мер, направленных на защиту информации в компьютерной сети.**

Рассмотрим некоторые методы защиты компьютерных систем от преднамеренных информационных угроз.

Защита от хищения информации обычно осуществляется с помощью специальных программных средств. Несанкционированное копирование и распространение программ и ценной компьютерной информации является кражей интеллектуальной собственности.

Защищаемые программы подвергаются предварительной обработке, приводящей исполняемый код программы в состояние, препятствующее его выполнению на «чужих» компьютерах (шифрование файлов, вставка парольной защиты, проверка компьютера по его уникальным характеристикам и т. п.). Другой пример защиты: для предотвращения несанкционированного доступа к информации в локальной сети вводят систему разграничения доступа как на аппаратном, так и на программном уровнях. В качестве аппаратного средства разграничения доступа может использоваться электронный ключ, подключаемый, например, в разъем принтера.

Для защиты от компьютерных вирусов применяются «иммуностойкие» программные средства (программы-анализаторы), предусматривающие разграничение доступа, самоконтроль и самовосстановление. Антивирусные средства являются самыми распространенными средствами защиты информации.

В качестве физической защиты компьютерных систем используется специальная аппаратура, позволяющая выявить устройства промышленного шпионажа, исключить запись или ретрансляцию излучений компьютера, а также речевых и других несущих информацию сигналов. Это позволяет предотвратить утечку информативных электромагнитных сигналов за пределы охраняемой территории. Наиболее эффективным средством защиты информации в каналах связи является применение специальных протоколов и криптографии (шифрования).

Для защиты информации от случайных информационных угроз, например, в компьютерных системах, применяются средства повышения надежности аппаратуры:

- повышение надежности работы электронных и механических узлов и элементов;
- структурная избыточность — дублирование или утроение элементов, устройств, подсистем;
- функциональный контроль с диагностикой отказов, то есть обнаружение сбоев, неисправностей и программных ошибок и исключение их влияния на процесс обработки информации, а также указание места отказавшего элемента.

С каждым годом количество угроз информационной безопасности компьютерных систем и способов их реализации постоянно увеличивается. Основными причинами здесь являются недостатки современных информационных технологий и постоянно возрастающая сложность аппаратной части. На преодоление этих причин направлены усилия многочисленных разработчиков программных и аппаратных методов защиты информации в компьютерных системах.

Контрольные задания:

1.Перейдите по ссылке, изучите материал, выпишите основные положения
http://infdeyatchel.narod.ru/_private/metodik/urok/prav_norm.swf

2. Ответьте на следующие вопросы:

1. Кто следит за порядком в сети?
2. Какие есть требования к защите информации?
3. Какими правами обладает пользователь?
4. Как владелец может защитить?
5. Что такое информационное право?

6. Какие есть акты федерального законодательства?

7. Какие есть способы защиты информации?

8. Какие есть наказания за информационные правонарушения?

9. Какие есть самые грубые нарушения в сфере информационной безопасности?

3. Сделать вывод о проделанной практической работе: