**Министерство науки и высшего образования Российской Федерации**

**Федеральное государственное автономное образовательное учреждение высшего образования**

**«Самарский государственный экономический университет»**

**Институт** Экономики предприятия

**Кафедра** Прикладная информатика

**Практическая работа**

**«Правовые нормы в информационной деятельности»**

по дисциплине

«Цифровая культура в профессиональной деятельности»

Выполнил:

Пауков Владислав Денисович

ИЦСУ25о2

Проверил:

Яшин Валерий Вадимович

Самара 2025

**Цель:** Изучить правовые нормы в информационной деятельности человека.

**Краткое описание теории:**

**Правовое регулирование**

Право собственности состоит из трех важных компонентов:

♦ 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.

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.

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

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
* 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
* 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 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.

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.

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

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 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.

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.

**Выполнение работы:**

1. Кто следит за порядком в сети?

Гос органы (МВД, ФСБ и тд),

Администраторы сетей

Провайдеры

1. Какие есть требования к защите информации?

Конфиденциальность

Целостность

Доступность

Правомерность сбора данных

1. Какими правами обладает пользователь?

Право на доступ информации, на защиту личных данных, на использование информации в законных целях

1. Как владелец может защитить?

Использовать пароли, шифрование

Обновлять ПО и антивирус

Установить права доступа

1. Что такое информационное право?

Совокупность правовых норм, регулирующих отношение в сфере получения, хранения, использования и защиты информации

1. Какие есть акты федерального законодательства?

Конституция РФ (ст. 23, 24, 29 – права на тайну переписки)

Федеральный закон об информации, информационных технологиях и о защите информации

УК РФ ст 272-274 – компьютерные преступления

1. Какие есть способы защиты информации?

Технические (шифрования, антивирус, файрвол)

Организационные (Регламенты, обучение сотрудников и тд)

1. Какие есть наказания за информационные правонарушения?

Административные штрафы

Уголовная ответственность

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

Взлом

Распространение вредоносного ПО

Кража и утечка персональных данных

DDoS

Распространение экстремистских материалов

**Вывод о проделанной практической работе №2**

В ходе работы я изучил правовые нормы в информационной деятельности человека, узнал кто следит за порядком в сети, как защищать информацию, изучил акты федерального законодательства,