

Правовые нормы, относящиеся к информации, правонарушения в информационной сфере, меры их предупреждения

Правовые нормы, относящиеся к информации

Содержание

1. Введение
2. Правовые нормы, относящиеся к информации.
3. Правонарушения в информационной сфере.
4. Меры предупреждения правонарушений в информационной сфере.
5. Заключение
6. Список использованных информационных ресурсов
7. Приложение

ВВЕДЕНИЕ

Информация является объектом правового регулирования.

Информация не является материальным объектом, но она фиксируется на материальных носителях. Первоначально информация находится в памяти человека, а затем она отчуждается и переносится на материальные носители: книги, диски, кассеты и прочие накопители, предназначенные для хранения информации. Как следствие, информация может тиражироваться путем распространения материального носителя. Перемещение такого материального носителя от субъекта-владельца, создающего конкретную информацию, к субъекту-пользователю влечет за собой утрату права собственности у владельца информации.

ВВЕДЕНИЕ

Интенсивность этого процесса существенно возросла в связи с распространением сети Интернет. Ни для кого не секрет, что очень часто книги, музыка и другие продукты интеллектуальной деятельности человека безо всякого на то согласия авторов или издательств размещаются на различных сайтах без ссылок на первоначальный источник. Созданный ими интеллектуальный продукт становится достоянием множества людей, которые пользуются им безвозмездно, и при этом не учитываются интересы тех, кто его создавал. 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.

*Правовые
нормы,
относящиеся к
информации*

Правовые нормы, относящиеся к информации

Законодательные акты РФ

Закон РФ №3523-1 «О правовой охране программ для ЭВМ и баз данных» дает юридически точное определение понятий, связанных с авторством и распространением компьютерных программ и баз данных. Он определяет, что авторское право распространяется на указанные объекты, являющиеся результатом творческой деятельности автора. Автор имеет исключительное право на выпуск в свет программ и баз данных, их распространение, модификацию и иное использование.

Правовые нормы, относящиеся к информации

Закон Российской Федерации №149-ФЗ «Об информации, информационных технологиях и защите информации» (рис. 1) регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу и производство информации;
- применении информационных технологий;
- обеспечении защиты информации.

Правовые нормы, относящиеся к информации

В 1996 году в Уголовный кодекс был впервые внесен раздел «Преступления в сфере компьютерной информации». Он определил меру наказания за некоторые виды преступлений, ставших распространенными:

- неправомерный доступ к компьютерной информации;
- создание, использование и распространение вредоносных программ для ЭВМ;
- умышленное нарушение правил эксплуатации ЭВМ и сетей.

Правовые нормы защиты информации

В 2002 году был принят закон «Об электронно-цифровой подписи», который стал законодательной основой электронного документооборота в России.

В 2006 году вступил в силу закон №152-ФЗ «О персональных данных» (рис. 2), целью которого является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных (с использованием средств автоматизации или без использования таких) в том числе защиты прав на неприкосновенность частной жизни.

*Правонарушения в
информационной
сфере*

Правонарушения в информационной сфере

Правонарушение – юридический факт (наряду с событием и действием), действия, противоречащие нормам права (антипод правомерному поведению). Правонарушения всегда связаны с нарушением определенным лицом (лицами) действующей нормы (норм) ИП и прав других субъектов информационных правоотношений. При этом эти нарушения являются общественно опасными и могут влечь для тех или иных субъектов трудности, дополнительные права и обязанности.

Правонарушения в информационной сфере

Преступления в сфере информационных технологий включают:

- распространение вредоносных вирусов;
- взлом паролей;
- кражу номеров кредитных карточек и других банковских реквизитов;
- распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и т. п.) через Интернет.

Правонарушения в информационной сфере

Основные правонарушения:

- ❖ пиратское копирование и распространение;
- ❖ несанкционированный доступ;
- ❖ изменение или уничтожение информации (негативные последствия в медицине, оборонной, атомной промышленности);
- ❖ распространение вирусных программ;
- ❖ компьютерное мошенничество (похищение и использование паролей, похищение банковских реквизитов).

Правонарушения в информационной сфере

Классификация компьютерных преступлений

❑ Преступления, связанные с вмешательством в работу ПК

❑ Преступления, использующие ПК в качестве «средства» достижения цели



*Меры предупреждения
правонарушений в
информационной сфере*

Меры предупреждения правонарушений в информационной сфере

К мерам относятся:


- охрана вычислительного центра;
- тщательный подбор персонала;
- исключение случаев ведения особо важных работ только одним человеком;
- наличие плана восстановления работоспособности центра после выхода его из строя;

Меры предупреждения правонарушений в информационной сфере

К мерам относятся:

- организация обслуживания вычислительного центра посторонней организацией или людьми;
- универсальность средств защиты от всех пользователей;
- возложение ответственности на лиц, которые должны обеспечить безопасность центра;
- выбор места расположения центра и т.п.





Меры предупреждения правонарушений в информационной сфере

А так же:

разработка норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства.

Меры предупреждения правонарушений в информационной сфере

Методы защиты информации:

- криптографическое закрытие информации;
- шифрование;
- аппаратные методы защиты;
- программные методы защиты;

- резервное копирование;
- физические меры защиты;
- организационные меры(табл. 1).

1. Криптографическое закрытие информации

- 1) выбор рациональных систем шифрования для надёжного закрытия информации;
- 2) обоснование путей реализации систем шифрования в автоматизированных системах;
- 3) разработка правил использования криптографических методов защиты в процессе функционирования автоматизированных систем;
- 4) оценка эффективности криптографической защиты.

2. Шифрование

Шифрование заменой (иногда употребляется термин «подстановка») заключается в том, что символы шифруемого текста заменяются символами другого или того же алфавита в соответствии с заранее обусловленной схемой замены.



3. Аппаратные методы защиты

- специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;
- генераторы кодов, предназначенные для автоматического генерирования идентифицирующего кода устройства;
- устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;





3. Аппаратные методы защиты

- специальные биты секретности, значение которых определяет уровень секретности информации, хранимой в ЗУ, которой принадлежат данные биты;
- схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.





4. Программные методы защиты

- ✓ идентификация технических средств (терминалов, устройств группового управления вводом-выводом, ЭВМ, носителей информации), задач и пользователей;
- ✓ определение прав технических средств (дни и время работы, разрешенная к использованию задачи) и пользователей;
- ✓ контроль работы технических средств и пользователей;
- ✓ регистрация работы технических средств и пользователей при обработке информации ограниченного использования.





4. Программные методы защиты

- ✓ уничтожение информации в ЗУ после использования;
- ✓ сигнализации при несанкционированных действиях;
- ✓ вспомогательные программы различного значения: контроля работы механизма защиты, проставление грифа секретности на выдаваемых документах.

5. Резервное копирование

- ❖ заключается в хранение копии программ в носителе: стримере, гибких носителях оптических дисках, жестких дисках;
- ❖ проводится для сохранения программ от повреждений (как умышленных, так и случайных), и для хранения редко используемых файлов.

6. Физические меры защиты

- физическая изоляция сооружений, в которых устанавливается аппаратура автоматизированной системы, от других сооружений;
- ограждение территории вычислительных центров заборами на таких расстояниях, которые достаточно для исключения эффективной регистрации электромагнитных излучений, и организации систематического контроля этих территорий;





6. Физические меры защиты

- организация контрольно-пропускных пунктов у входов в помещения вычислительных центров или оборудованных входных дверей специальными замками, позволяющими регулировать доступ в помещения;
- организация системы охранной сигнализации.



7. Организационные меры

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров (ВЦ)
- мероприятия, осуществляемые при подборе и подготовке персонала ВЦ (проверка принимаемых на работу, создание условий при которых персонал не хотел бы лишиться работы, ознакомление с мерами ответственности за нарушение правил защиты);





7. Организационные меры

- организация надежного пропускного режима;
- организация хранения и использования документов и носителей: определение правил выдачи, ведение журналов выдачи и использования;
- контроль внесения изменений в математическое и программное обеспечение;
- организация подготовки и контроля работы пользователей.

Причины защиты информации

1. Резкое объемов информации, накапливаемой, хранимой и обрабатываемой с помощью ЭВМ и других средств автоматизации.
2. Сосредоточение в единых базах данных информации различного назначения и различных принадлежностей.
3. Резкое расширение круга пользователей, имеющих непосредственный доступ к ресурсам вычислительной системы и находящимся в БИХ.



Причины защиты информации



4. Усложнение режимов функционирования технических средств вычислительных систем: широкое внедрение многопрограммного режима, а также режимов разделения времени и реального мира.
5. Автоматизация межмашинного обмена информацией, в том числе и на больших расстояниях.

Заключение

В связи с возрастающим значением информационных ресурсов предприняты ряд правовых мер для их охраны и защиты. Многие черты информационного общества уже присутствуют в современной жизни развитых стран. Жизненно важной для общества становится проблема информационной безопасности действующих систем хранения, передачи и обработки информации.

Заключение

Компьютеры контролируют работу атомных реакторов, распределяют электроэнергию, управляют самолётами и космическими кораблями, определяют надёжность систем обороны страны и банковских систем, т.е. используются в областях общественной жизни, обеспечивающих благополучие и даже жизнь множества людей. О важности проблемы информационно безопасности свидетельствуют многочисленные факты. Более 80% компьютерных преступлений осуществляется через глобальную сеть Интернет, которая обеспечивает широкие возможности злоумышленникам для нарушений в глобальном масштабе.

Список использованных информационных ресурсов

1. http://emit.do.am/index/tema_1_2/0-46
2. http://tov2015.ucoz.ru/index/pravovye_normy/0-72
3. http://infourok.ru/komplekt_lekciy_po_uchebnoy_discipline_informatika_i_ikt-510940.htm
4. Бондаренко Е. А., Журин А. А., Милютин И. А. Технические средства обучения в современной школе: Пособие для учителя и директора школы. / Под ред. А. А. Журин. – М.: «ЮНВЕС», 2004. – 416 с.
5. Захарова И. Г. Информационные технологии в образовании: Учебн. пособие для высш. учебн. заведений. – М.: Издательский центр «Академия», 2005. – 192 с.

Приложение



Рис.1 Закон Российской Федерации №149-ФЗ «Об информации, информационных технологиях и защите информации»



Рис.2 Закон №152-ФЗ «О персональных данных»

Табл. 1 Методы защиты информации





**СПАСИБО ЗА
ВНИМАНИЕ!!!**