Лекция 10. ИТ и право. Технологии компьютерных преступлений (1,2)

Лекция 11. Меры защиты информационной безопасности. Физическая безопасность (3,4)

ПЛАН:

1. Информационные технологии и право
2. Технологии компьютерных преступлений
3. Меры защиты информационной безопасности
4. Физическая безопасность

1. Информационные технологии и право

КОМПЬЮТЕРНОЕ ПРАВО -

новая отрасль законодательства РФ, представляющая совокупность правовых норм, регулирующих комплекс общественных отношений, возникающих в процессе эксплуатации ЭВМ, системы ЭВМ или их сети.

Законодательство России в области компьютерного права начало формироваться с конца 1991 года и включает 9 основных законов:

1. Закон «О средствах массовой информации» (27.12.91 г. N 2124-I)

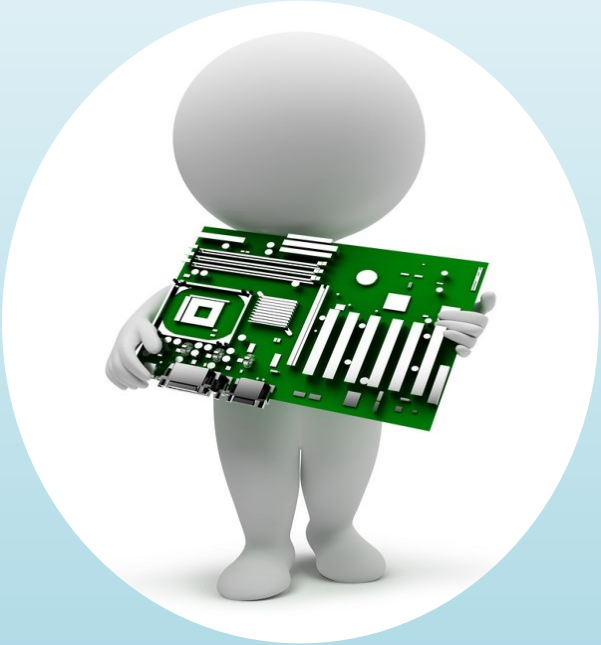
Исходя из ст.2 правомерно предположить, что средства массовой информации могут создаваться и распространяться не только с помощью печатных изданий, теле-, видеопрограмм, но и с использованием новых информационных технологий.

2. Патентный закон РФ (от 23.09.92 г. N 3517-I)

Создает механизмы защиты отдельных элементов новых информационных технологий, в первую очередь, технических средств вычислительной техники и телекоммуникационного оборудования, как объектов промышленной собственности.

3. Закон «О правовой охране топологий интегральных микросхем» (от 23.09.92 г. N 3526-I)

Создает систему правового регулирования отношений, возникающих при создании, правовой охране и использовании топологий интегральных микросхем.



Интегральная микросхема (ИМС) является основным электронным элементом компьютера.

4. Закон «О правовой охране программ для электронных вычислительных машин и баз данных» (от 23.09.92 г. N 3523-I)

Регулирует исключительные авторские права на программы для ЭВМ и базы данных (как личные, так и имущественные)

Программам для ЭВМ предоставляется правовая охрана как произведениям литературы, а базам данных – как сборникам.»

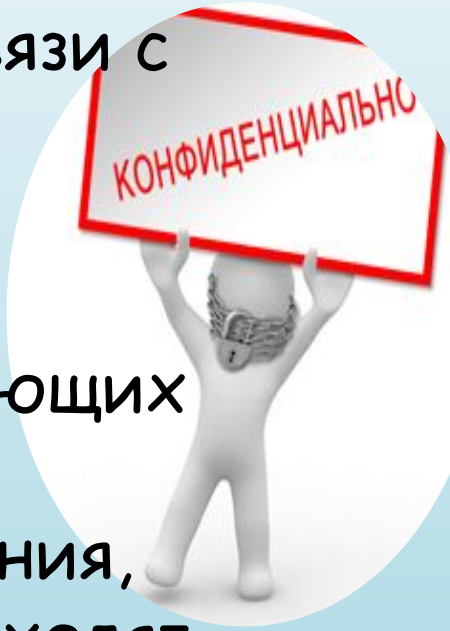
5. Закон «Об авторском праве и смежных правах» (от 9.07.93 г. N 5351-I)

В отношении программ для ЭВМ и баз данных рассматриваемый закон как более поздний вносит ряд уточнений:

- не допускается воспроизведение программ для ЭВМ в личных целях без согласия автора и без выплаты авторского вознаграждения (ст. 18);
- установлены правила свободного воспроизведения программ для ЭВМ и баз данных, декомпилирования программ для ЭВМ (ст. 25).

6. Закон «О государственной тайне» (от 21.07.93 г. N 5485-I)

Регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности РФ.



В качестве носителей сведений, составляющих государственную тайну, рассматриваются «материальные объекты, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов».

В связи с этим закон применяется и к сведениям, составляющим государственную тайну и хранимым в памяти ЭВМ.

7. Закон «Об обязательном экземпляре документов» (от 29.12.94 г. N 77-ФЗ)

Согласно ст. 5, в числе документов, входящих в состав обязательного бесплатного экземпляра и обязательного платного экземпляра, указаны «электронные издания, включающие программы для ЭВМ и базы данных или представляющие собой программы для ЭВМ и базы данных».

8. Закон «О связи» (от 16.02.95 г. N 15-ФЗ)

Регулирует обширную область правоотношений, возникающих при передаче информации по каналам связи (при осуществлении удаленного доступа пользователей к базам данных, обмене электронными сообщениями и других ситуациях).

9.Закон «Об информации, информатизации и защите информации» (от 20.02.95 г. N 24-ФЗ).

Важнейшим элементом реализуемой в законе концепции является объявление информационных ресурсов объектом права собственности и включение их в состав имущества (ст. 6). Устанавливается право собственности на отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (ст. 4), а также право собственности на информационные системы, технологии и средства их обеспечения (ст. 17).

2. Технологии компьютерных преступлений

Основные виды преступлений, связанных с вмешательством в работу компьютеров:

1) Несанкционированный доступ к информации, хранящейся в компьютере. Осуществляется с использованием чужого имени, изменением физических адресов технических устройств.

2) Ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему.

Основные методы, использовавшиеся для совершения компьютерных преступлений:

3) Разработка и распространение компьютерных вирусов.
"Троянские кони" обладают свойствами переходить через коммуникационные сети из одной системы в другую, распространяясь как вирусное заболевание.

4) Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям.

Основные методы, использовавшиеся для совершения компьютерных преступлений:

5) Подделка компьютерной информации.

К подделке информации можно отнести также подтасовку результатов выборов, голосований, референдумов и т.п.

6) Хищение компьютерной информации.

3. Меры защиты информационной безопасности

 Контролировать доступ как к информации в компьютере, так и к прикладным программам:

1. Идентификация пользователей;
2. Аутентификация пользователей;
3. Защищать пароль;
4. Серьезно относиться к администрированию паролей;
5. Разработка процедуры авторизации;
6. Защита файлов;
7. Предосторожности при работе.

 Защищать целостность информации.

1. Проверять точность информации;
2. Проверять точность вводимых данных;
3. Проводить проверки на корректность связей с другими данными;
4. Проводить проверки на разумность.

 Защищать системные программы.

Если ПО используется совместно, защищать его от скрытой модификации при помощи политики безопасности, мер защиты при его разработке и контроле за ним в его жизненном цикле, а также обучения пользователей в области безопасности.

1. Должен быть разработан и поддерживаться каталог прикладных программ.
2. Должны быть внедрены меры защиты по предотвращению получения, изменения или добавления программ неавторизованными людьми через удаленные терминалы.

 Сделать меры защиты более адекватными с помощью привлечения организаций, занимающихся тестированием информационной безопасности.

Должны иметься контрольные журналы для наблюдения за тем, кто из пользователей обновлял критические информационные файлы..

 Рассмотреть вопрос о коммуникационной безопасности.

Данные, передаваемые по незащищенным линиям, могут быть перехвачены.

3. Меры защиты информационной безопасности

 Контролировать доступ как к информации в компьютере, так и к прикладным программам:

1. Идентификация пользователей;
2. Аутентификация пользователей;
3. Защищать пароль;
4. Серьезно относиться к администрированию паролей:
5. Разработка процедуры авторизации;
6. Защита файлов;
7. Предосторожности при работе.

4. ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

 Нормативное обеспечение

1. Разработать, задокументировать и периодически обновлять политики физической защиты и защиты среды информационной системы;
2. Необходимо разработать процедуры и меры, связанные с реализацией политики физической защиты и защиты средств информационной системы.

Персонал и уровни доступа

1. Необходимо разработать списки персонала, которым будет разрешен доступ в соответствии с политикой безопасности, а также механизм идентификации (бейджи, информационные карты и т.п.);

2. Соответствующие должностные лица должны рассматривать и утверждать списки доступа, а также пересматривать списки в соответствии с установленной периодичностью.

Управление физическим доступом

1. Необходимо иметь систему правления доступом во всех точках доступа к информационным ресурсам и активам

2. Доступ в помещения и здания должен быть предоставлен только авторизованному персоналу

3. Необходимо регулярно анализировать и пересматривать права доступа сотрудников в зоны безопасности

Мониторинг физического доступа

1. В процессе мониторинга должны использоваться устройства наблюдения и сигнализации реального времени

2. Контроль физического доступа к помещениям должен обеспечиваться использованием самых жестких методов идентификации/аутенти фикации

Защита оборудования

1. Оборудование необходимо защищать от перебоев в подаче электроэнергии

2. Необходимо обеспечить противопожарную защиту, а также защиту от других экологических и техногенных катастроф

3. Необходимо защищать телекоммуникационные кабельные сети от пере-хвата информации или повреждения

Контроль посетителей

1. Должна быть выделена зона регистрации посетителей

2. Должны вестись журналы учета доступа посетителей

3. Должны использоваться автоматизированные средства ведения журналов учета доступа посетителей

Ответить на вопросы теста!

1. **Какой закон существуют в России в области компьютерного права?**
   a. о гражданском долге;
   b. о правовой ответственности;
   c. об информации, информатизации, защищенности информации.
2. **Что называют защитой информации?**
   a. все ответы верны;
   b. деятельность по предотвращению утечки защищаемой информации ;
   c. деятельность по предотвращению несанкционированных воздействий на защищаемую информацию;
   d. деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию.
3. **Потенциальные угрозы, против которых направлены технические меры защиты информации:**
   a. потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей;
   b. потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения;
   c. процессы преобразования, при котором информация удаляется.

4. **Назначение пароля в ИС?**
   a. скрытие копирования участков магнитной ленты из ОЗУ в ПЗУ;
   b. механизм управления доступом, средство защиты и безопасность личной информации;
   c. технические меры защиты и средство защиты данных.
5. **Троянской программой является...**
   a. программа, вредоносное действие которой выражается в удалении и/или модификации системных файлов компьютера;
   b. программа, заражающая компьютер независимо от действий пользователя;
   c. вредоносная программа, которая сама не размножается, а выдает себя за что-то полезное, тем самым пытаясь побудить пользователя переписать и установить на свой компьютер программу самостоятельно