Презентация подготовлена для конкурса «Интернешка».
http://interneshka.org/.

Ученика 11 (А) класса средней общеобразовательной школы МБОУ №149 Бердникова Артёма.

На тему: **«Правовые и этические аспекты использования интернета».**

Самара, 2015

Но́рма пра́ва — это общеобязательное, формально определенное правило поведения, гарантируемое государством, отражающее уровень свободы гражданина и выступающее регулятором общественных отношений.

Этические нормы - нравственные правила, соблюдение которых организация требует от своих сотрудников.

Правовые вопросы использования интернета.

1. Защита частной жизни.

Рассматривает вопросы:

- При каких обстоятельствах разрешен сбор информации? Например, заполняя заявку на участие в лотерее или конкурсе, потребитель предоставляет свою частную информацию. Может ли компания хранить ее или продавать?
- Если частная информация собрана без согласия клиента, законно ли ее хранить или продавать? Например, cookies могут дать сведения о вкусах и предпочтениях потребителя.
- Как можно обеспечить контроль пользователей Интернет за использованием переданной ими информации?
- Если пользователи Интернет предоставляют свой электронный адрес, можно ли его автоматически вносить в список рассылки? Или обязательно запрашивать их согласия?

2. Защита прав собственности.

Включает:
- интеллектуальную собственность;
- защиту электронной собственности, т.е. собственности в цифровом формате.

- Как собственникам и провайдерам таких продуктов защитить себя от их незаконного копирования и использования?

- Как защитить авторские права и патенты на электронные продукты?

- Многие программные продукты сейчас можно приобрести непосредственно в сети, а не дискетах или дисках. Достаточно лишь подписать согласие соблюдать установленные правила использования и оплатить продукт. Как собственникам этих товаров защитить себя от незаконного копирования и тиражирования без оплаты?

3. Свобода слова.

Интернет дает самые широкие возможности для свободы слова. Но эта свобода слова для одних граждан может быть оскорбительна для других.

- Какие законные акты регулируют свободу слова в Интернет и защищают потребителей от порнографии и неэтичного маркетинга?

4. Налогообложение электронной коммерции.

- различия в налоговом законодательстве разных стран.

Интернет не имеет национальных границ, сложно определить, в юрисдикции каких налоговых органов находится конкретная сделка. Гражданин одной страны нарушил
закон другой страны. Однако в родной стране нарушителя такого закона нет.

- Законы какой страны следует применять?

Комиссия ООН по международному торговому праву подготовила образец закона об электронной коммерции, стремясь установить единые международные стандарты в этой области. Любая компания, занимающаяся электронной коммерцией за пределами своей страны, должна быть осведомлена о действующих в других странах законах и ограничениях.

Этические вопросы использования интернета.

1. Защита частной жизни (сбор, хранение распространение информации о частных лицах).

2. Точность информации (аутентичность, надежность точность собранной и обработанной информации).

3. Защита прав собственности (права собственности стоимость информации, защита интеллектуальн собственности).

4. Доступ к информации (права доступа информации и оплата такого доступа).

Этические и правовые аспекты информационной деятельности. Правовая охрана программ и данных. Защита информации.

Юридические статусы программ.

- лицензионные;
- условно бесплатные (shareware);
- свободно распространяемые (freeware).

Свободно распространяемые:

• новые недоработанные (бета) версии программных продуктов (позволяет провести их широкое тестирование);

•программные продукты, являющиеся частью принципиально новых технологий (позволяет завоевать рынок);

•дополнения к ранее выпущенным программам, исправляющие найденные ошибки или расширяющие возможности;

•устаревшие версии программ;

•драйверы к новым устройствам или улучшенные драйверы к уже существующим.

Правовая охрана информации.

Правовая охрана программ и баз данных впервые в полном объеме введена в Российской Федерации Законом РФ «О правовой охране программ для электронных вычислительных машин и баз данных», который вступил в силу в 1992 году.

Для оповещения о своих правах разработчик программы может, начиная с первого выпуска в свет программы, использовать знак охраны авторского права, состоящий из трех элементов:
буквы С в окружности или круглых скобках ©;
наименования (имени) правообладателя;
года первого выпуска программы в свет.

Например, знак охраны авторских прав на текстовый редактор Word выглядит следующим образом:
© Корпорация Microsoft, 1993-1997.

Электронная подпись.

В 2002 году был принят Закон РФ «Об электронно-цифровой подписи», который стал законодательной основой электронного документооборота в России. По этому закону электронная цифровая подпись в электронном документе признается юридически равнозначной подписи в документе на бумажном носителе.

При регистрации электронно-цифровой подписи в специализированных центрах корреспондент получает два ключа: секретный и открытый. Секретный ключ хранится на дискете или смарт-карте и должен быть известен только самому корреспонденту. Открытый ключ должен быть у всех потенциальных получателей документов и обычно рассылается по электронной почте.

Процесс электронного подписания документа состоит в обработке с помощью секретного ключа текста сообщения. Далее зашифрованное сообщение посылается по электронной почте абоненту. Для проверки подлинности сообщения и электронной подписи абонент использует открытый ключ.

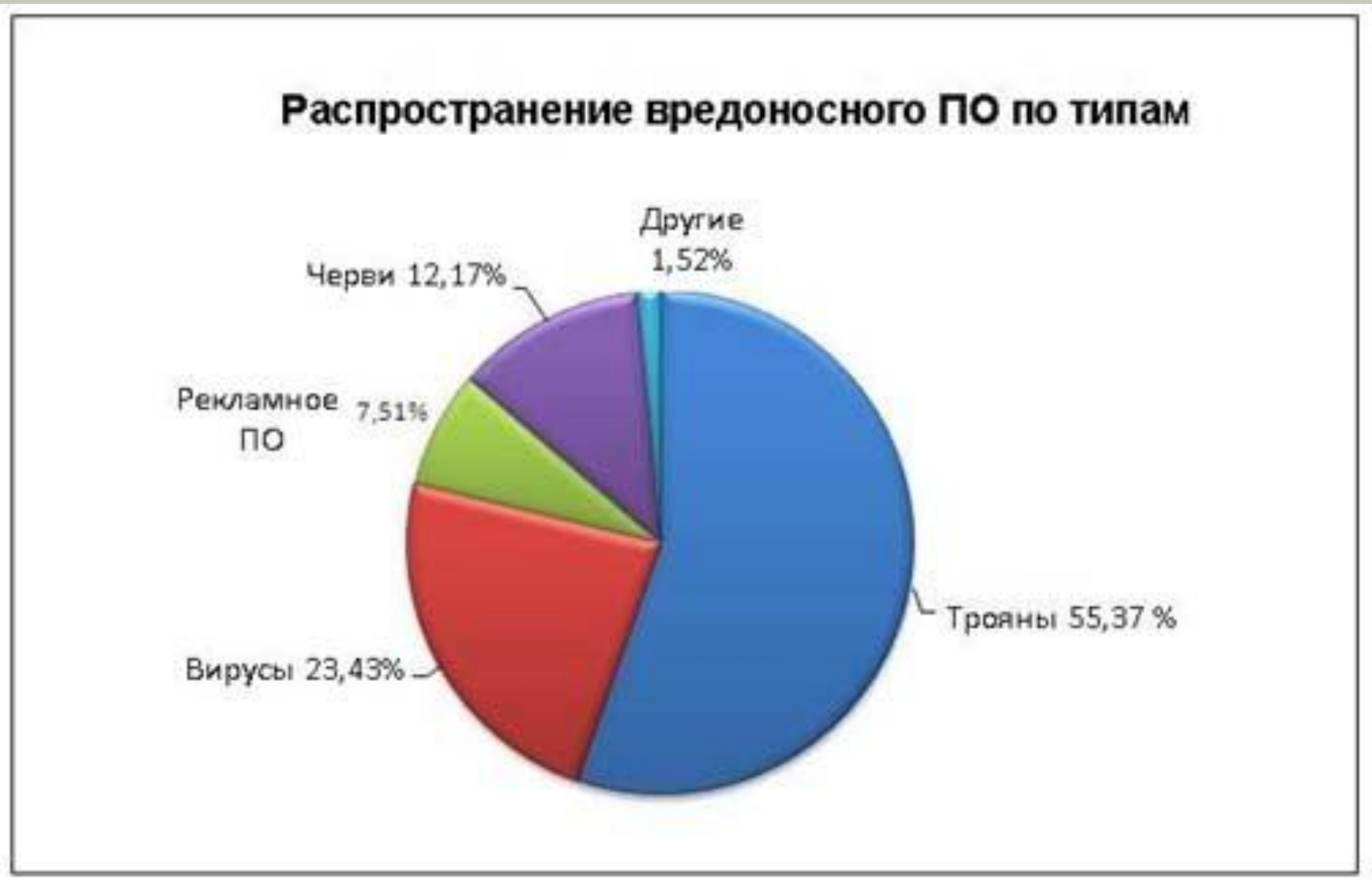
Защита информации в Интернете

- если компьютер подключен к Интернету, то любой пользователь, также подключенный к Интернету, может получить доступ к информационным ресурсам этого компьютера.
- если сервер имеет соединение с Интернетом и одновременно служит сервером локальной сети (Интранет-сервером), то возможно несанкционированное проникновение из Интернета в локальную сеть.

Механизмы проникновения из Интернета на локальный компьютер и в локальную сеть :

- загружаемые в браузер Web-страницы могут содержать активные элементы ActiveX или Java-апплеты, способные выполнять деструктивные действия на локальном компьютере;
- некоторые Web-серверы размещают на локальном компьютере текстовые файлы cookie, используя которые можно получить конфиденциальную информацию о пользователе локального компьютера;
- с помощью специальных утилит можно получить доступ к дискам и файлам локального компьютера и др.

Устанавливается программный или аппаратный барьер между Интернетом и Интранетом с помощью брандмауэра (firewall — межсетевой экран).
Брандмауэр отслеживает передачу данных между сетями, осуществляет контроль текущих соединений, выявляет подозрительные действия и предотвращает несанкционированный доступ из Интернета в локальную сеть.


Распространение вредоносного ПО по типам
Другие 1,52%
Черви 12,17%
Рекламное ПО 7,51%
Вирусы 23,43%
Трояны 55,37 %

Борьба с интернет-преступлениями со стороны государства:

Управления «К» БСТМ МВД России:

Основные направления работы

1. Борьба с преступлениями в сфере компьютерной информации:
- выявление и пресечение фактов неправомерного доступа к компьютерной информации;
- борьба с изготовлением, распространением и использованием вредоносных программ для ЭВМ;
- противодействие мошенническим действиям с использованием возможностей электронных платежных систем;
- борьба с распространением порнографических материалов с участием несовершеннолетних через сеть Интернет.

2. Пресечение противоправных действий в информационно- телекоммуникационных сетях, включая сеть Интернет:
- выявление и пресечение преступлений, связанных с незаконным использованием ресурсов сетей сотовой и проводной связи;
- противодействие мошенническим действиям, совершаемым с использованием информационно-телекоммуникационных сетей, включая сеть Интернет;
- противодействие и пресечение попыток неправомерного доступа к коммерческим каналам спутникового и кабельного телевидения.

3. Борьба с незаконным оборотом радиоэлектронных и специальных технических средств.

4. Выявление и пресечение фактов нарушения авторских и смежных прав в сфере информационных технологий.

5. Борьба с международными преступлениями в сфере информационных технологий:
- противодействие преступлениям в сфере информационных технологий, носящим международный характер;
- взаимодействие с национальными контактными пунктами зарубежных государств.

6. Международное сотрудничество в области борьбы с преступлениями, совершаемыми с использованием информационных технологий.

БСТМ МВД России активно взаимодействует с правоохранительными органами иностранных государств как на двусторонней, так и многосторонней основе (ООН, «восьмерка», СНГ, СЕ, ЕС, ШОС, АТР и др.).