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

Информация является **объектом правового регулирования**. Информация не является материальным объектом, но она фиксируется на материальных носителях.

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

Авторское право — отрасль гражданского права, регулирующая правоотношения, касающиеся интеллектуальной собственности.

Система источников авторского права представляет достаточно целостную совокупность законодательных актов, регулирующих авторские отношения, связанные с созданием и использованием произведений науки, литературы и искусства.

Правовые нормы, относящиеся к информации

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.

Правовые нормы, относящиеся к информации

Любой субъект - **пользователь обязан приобрести эти права**, прежде чем воспользоваться интересующим его информационным продуктом.

Любой закон о праве собственности регулирует отношения между субъектом-владельцем и субъектом-пользователем.

Закон РФ №3523-I «О правовой охране программ для ЭВМ и баз данных» дает юридически точное определение понятий, связанных с авторством и распространением компьютерных программ и баз данных.

Правовые нормы, относящиеся к информации

Закон Российской Федерации №149-ФЗ «Об информации, информационных технологиях и защите информации» 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 №152-0ФЗ «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

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.
- изменение или уничтожение информации (негативные последствия в медицине, оборонной, атомной промышленности).

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:

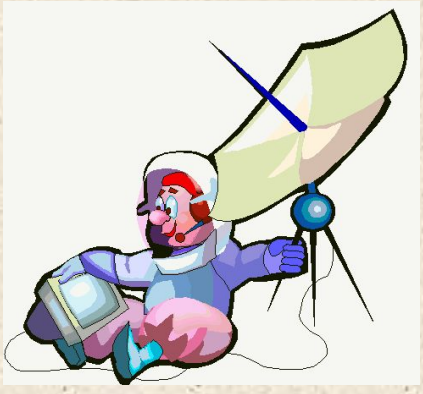
- криптографическое закрытие информации;
- шифрование;
- аппаратные методы защиты;
- программное методы защиты;
- резервное копирование;
- физические меры защиты;
- организационные меры.

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.

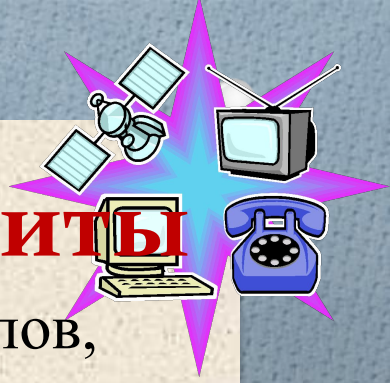


3. Аппаратные методы защиты

- 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, разрешенные к использованию задачи) и пользователей;
- контроль работы технических средств и пользователей;
- регистрация работы технических средств и пользователей при обработки информации ограниченного использования.

4. Программное 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 носителей 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 проектирование, строительстве и оборудовании вычислительных центров (ВЦ)
- мероприятия, осуществляемые при подборе и подготовки 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 ых.

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.

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.

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.

Электронное правительство -

Это способ предоставления информации и оказания уже сформировавшегося набора государственных услуг гражданам, бизнесу, другим ветвям государственной власти и государственным чиновникам, при котором личное взаимодействие между государством и заявителем минимизировано и максимально возможно используются информационные технологии.

Развитие информационного общества подталкивает многие организации к принятию концепции «электронного правительства» с целью:

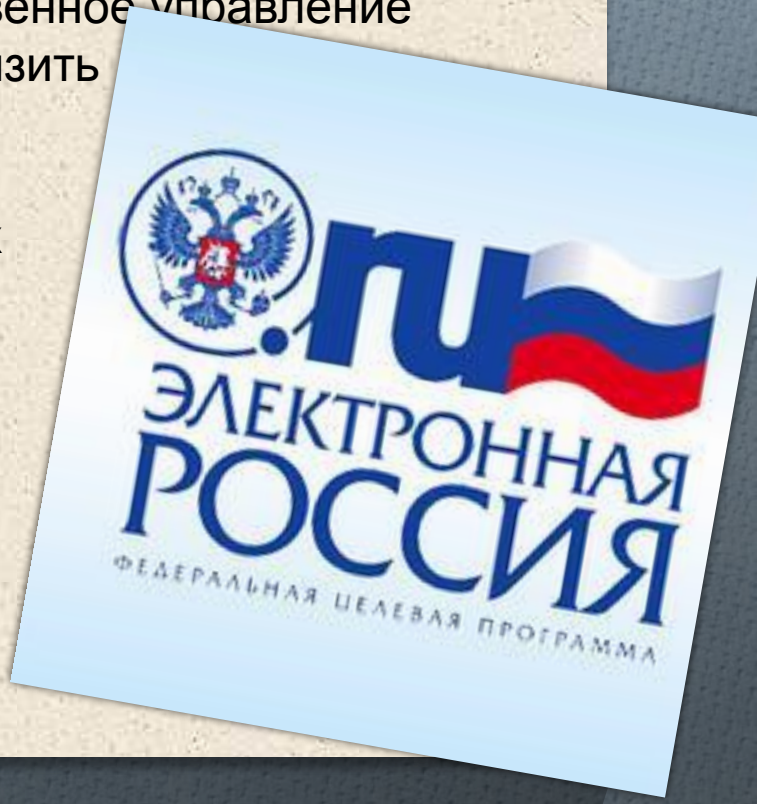
- ***Предоставлять услуги для населения в интегрированном виде по сети Интернет;***
- ***Преодолеть информационное неравенство:;***
- ***Дать людям возможность обучаться на протяжении всей жизни;***
- ***Перестроить взаимоотношения с населением;***
- ***Способствовать развитию экономики;***
- ***Выработать разумные законы и разумную политику;***
- ***Создать формы правления с большим участием граждан.***

Правительство должно быть доступно каждому, в любом месте, в любое время.

Цель создания электронного правительства состоит в том, что электронное правительство не является дополнением или аналогом традиционного правительства, а лишь определяет новый способ взаимодействия на основе активного использования информационно-коммуникационных технологий в целях повышения эффективности предоставления государственных услуг.

История создания электронных правительств

идет параллельно с развитием информационных технологий. Как полагают эксперты, введение информационно-коммуникационных технологий в государственное управление позволит ускорить развитие экономики, снизить затраты на бюрократические процедуры, повысить эффективность работы и производительность труда государственных ведомств, расширить возможности населения в формировании гражданского общества за счет улучшения доступа к различного рода информации, создания более прозрачной работы государственных служб, ослабления бюрократических барьеров.



Три стадии электронного правительства:

- Стадия 1 (публичность).
- Стадия 2 (онлайн-транзакции).
- Стадия 3 (участие).

Согласно концепции «**электронное правительство**» создавалось в два этапа:

2008 год - разработка и утверждение необходимых документов

2009-2013 годы - практическое внедрение

Взаимодействие с государственными органами по Интернету ещё более повышает конкурентоспособность частных компаний и даёт им возможность упростить различные официальные процедуры и количество канцелярской волокиты.

Государственные службы способны изменить к лучшему невысокое мнение населения о качестве оказываемых ими услуг и вновь обрести поддержку и доверие граждан.

«Электронное правительство», в самом полном смысле этого слова, — это та инфраструктура, которую сегодня создают государственные органы, чтобы изменить способы выполнения своих задач.

Переход к «электронному правительству» начинался с того, что различные организации начинали использовать Интернет:

1. Создавали веб-сайты;
2. Стали предоставлять информацию с возможностью для поиска по базам данных и службой ответов на послания по электронной почте;
3. Стали возможными предоставления финансовых и юридических услуг, чтобы граждане и частные фирмы могли покупать лицензии и разрешения, подавать налоговые декларации, платить штрафы за неправильную парковку и обращаться с просьбами о социальных льготах.

СПАСИБО ЗА ВНИМАНИЕ!!!