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

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.**

Правовое регулирование **— процесс целенаправленного воздействия государства на общественные отношения при помощи специальных юридических средств и методов, которые направлены на их стабилизацию и упорядочивание.**

Правовое регулирование является одним из составных элементов правового воздействия, которое по содержанию намного шире его и включает в себя не только целенаправленную деятельность по упорядочиванию общественных отношений, но и косвенное воздействие правовых средств и методов на субъектов непосредственно не подпадающих под правовое регулирование.

(НЕ пишем, только читаем!)

Правовое регулирование в информационной сфере является новой и сложной задачей для государства. В Российской Федерации существует ряд законов в этой области. Решение проблемы защиты информации во многом определяется теми задачами, которые решает пользователь, как специалист в конкретной области. В настоящее время для защиты от несанкционированного доступа к информации все более часто используются биометрические системы идентификации.

Используемые в этих системах характеристики являются неотъемлемыми качествами личности человека и поэтому не могут быть утерянными или поддельными.

Информационно-правовые нормы регулируют обособленную группу общественных отношений применительно к особенностям информационной сферы; задает содержание прав и обязанностей субъектов, участвующих в правоотношении.

Также регулируют взаимоотношения граждан, СМИ, организаций, фирм между собой, их взаимные права и обязанности.

Информационная безопасность Российской Федерации – состояние защищенности её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

(НЕ пишем, только читаем!)

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.

(НЕ пишем, только читаем!)

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.

(НЕ пишем, только читаем!)

О важности проблемы информационной безопасности свидетельствуют многочисленные факты. Более 80% компьютерных преступлений осуществляется через глобальную сеть Интернет, которая обеспечивает широкие возможности злоумышленникам для нарушений в глобальном масштабе.

Преступления в сфере информационных технологий, совершаемые людьми

Преступления в сфере информационных технологий включают как распространение вредоносных вирусов, взлом паролей, кражу номеров кредитных карточек и других банковских реквизитов, так и распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и т.п.) через Интернет.

Кроме того, одним из наиболее опасных и распространенных преступлений, совершаемых с использованием Интернета, является мошенничество.

(НЕ пишем, только читаем!)

Инвестирование денежных средств на иностранных фондовых рынках с использованием сети Интернет сопряжено с риском быть вовлеченными в различного рода мошеннические схемы. Другой пример мошенничества - интернет аукционы, в которых сами продавцы делают ставки, чтобы поднять цену выставленного на аукцион товара.

Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, серьёзное нарушение работы ЭВМ и их систем, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и с физическим вредом людям.

В соответствии с действующим уголовным законодательством Российской Федерации под преступлениями в сфере компьютерной информации понимаются *совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства.*

Правовое регулирование Российской Федерации

- ***закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных» (в ред. Федеральных законов от 24.12.2002 N 177-ФЗ, от 02.11.2004 N 127-ФЗ, от 02.02.2006 N 19-ФЗ)*** регламентирует юридические вопросы, связанные с авторскими правами на программные продукты и базы данных.
- ***закон РФ от 27 июля 2006 г. №149-ФЗ «Об информации, информатизации и защите информации»*** позволяет защищать информационные ресурсы (личные и общественные) от искажения, порчи, уничтожения.
- В ***Уголовном кодексе РФ*** имеется раздел «Преступления в сфере компьютерной информации». Он предусматривает наказания за:

1. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ);
2. Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ);
3. Умышленное нарушение правил эксплуатации ЭВМ и их сетей (ст. 274 УК РФ).

в **2006 году** вступил в силу **закон №152-0ФЗ «О персональных данных»**, 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.

Значимость безопасности информации

Прикладные задачи: сохранность личной информации пользователя

Управленческие задачи: обеспечение полноты управленческих документов

Информационные услуги: обеспечение доступности и безотказной работы

Коммерческая деятельность: предотвращение утечки информации

Банковская деятельность: обеспечение целостности информации

Факторы и условия, которые необходимо учитывать при разработке методов защиты информации

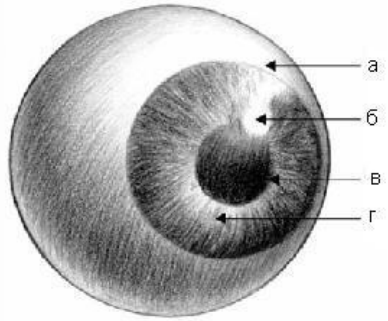
- Расширение областей использования компьютеров и увеличение темпа роста компьютерного парка
- Высокая степень концентрации информации в центрах ее обработки
- Расширение доступа пользователя к мировым информационным ресурсам
- Усложнение программного обеспечения вычислительного процесса на компьютере

Методы защиты информации
Шифрование (криптография) информации
Законодательные меры
Ограничение доступа к информации
Преобразование (кодирование) слов и т.д. с помощью специальных алгоритмов
Контроль доступа к аппаратуре
Вся аппаратура закрыта и в местах доступа к ней установлены датчики, которые срабатывают при вскрытии аппаратуры
На уровне среды обитания человека: выдача документов, установка сигнализации или системы видеонаблюдения
На уровне защиты компьютерных систем: введение паролей для пользователей

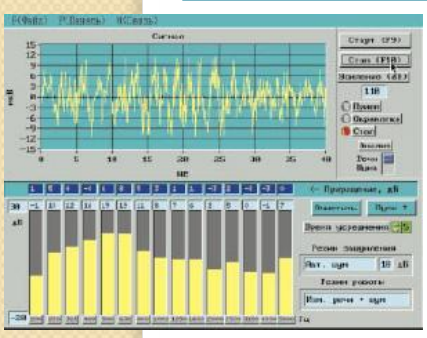
Биометрические системы защиты

По отпечаткам пальцев

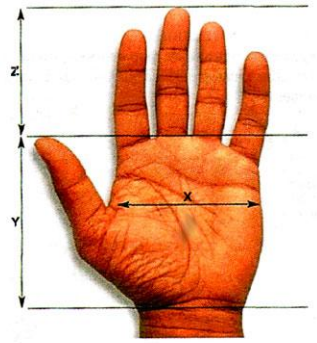
По радужной оболочке глаза



По характеристикам речи

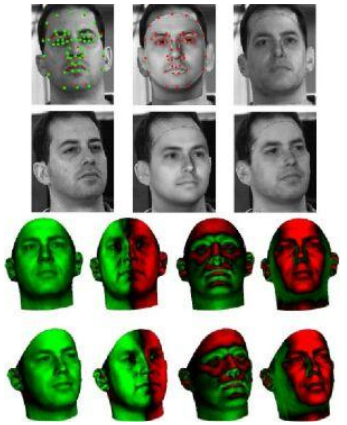


По геометрии ладони руки



X = ширина ладони, Y = длина ладони, Z = длина пальца

По изображению лица



ЗНАЧИМОСТЬ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
ПРИКЛАДНЫЕ ЗАДАЧИ
сохранность личной информации пользователя
УПРАВЛЕНЧЕСКИЕ ЗАДАЧИ
обеспечение полноты управленческих документов
ИНФОРМАЦИОННЫЕ УСЛУГИ
обеспечение доступности и безотказной работы
КОММЕРЧЕСКАЯ ДЕЯТЕЛБНОСТЬ
предотвращение утечки информации
БАНКОВСКАЯ ДЕЯТЕЛБНОСТЬ
обеспечение целостности информации

Лицензия (лицензионное соглашение) на программное обеспечение – это правовой инструмент, определяющий использование и распространение программного обеспечения. Лицензионное соглашение, как правило, регламентирует цели применения, например, только для обучения, и место применения, например, только для домашнего компьютера. Нарушение лицензионного соглашения является нарушением авторских прав и может повлечь за собой применение мер юридической ответственности. За нарушение авторских прав на программные продукты российским законодательством предусмотрена гражданско-правовая, административная и уголовная ответственность.

Электронное правительство *(англ. e-Government)* – система электронного документооборота государственного управления, основанная на автоматизации всей совокупности управленческих процессов в масштабах страны и служащая цели существенного повышения эффективности государственного управления и снижения издержек социальных коммуникаций для каждого члена общества.

Электронное правительство

(НЕ пишем, только читаем!)

Основная работа по формированию электронного правительства была начата с момента принятия *государственной программы Российской Федерации «Информационное общество (2011-2020 годы)», утверждённая распоряжением Правительства РФ от 20 октября 2010 г. № 1815-р*, в соответствии с которой был выполнен комплекс работ по формированию единой информационно-технологической и телекоммуникационной инфраструктуры электронного правительства.

Создание электронного правительства (ЭП) предполагает построение общегосударственной распределенной системы общественного управления, реализующей решение полного спектра задач, связанных с управлением документами и процессами их обработки.

ЭП не является дополнением или аналогом традиционного правительства, а лишь определяет новый способ взаимодействия на основе активного использования информационно-коммуникационных технологий (ИКТ) в целях повышения эффективности предоставления государственных услуг.

Домашнее задание

Расписать какие меры наказания предусматривает каждая статья ***Уголовного кодекса РФ*** в раздел «Преступления в сфере компьютерной информации»:

1. Неправомерный доступ к компьютерной информации (**ст. 272 УК РФ**);
2. Создание, использование и распространение вредоносных программ для ЭВМ (**ст. 273 УК РФ**);
3. Умышленное нарушение правил эксплуатации ЭВМ и их сетей (**ст. 274 УК РФ**).