

Правовое регулирование создания и применения ИТ

ПЛАН РАБОТЫ

- 1. Понятие и виды ИТ
- 2. Порядок создания ИТ
- 3. ИТ в применении некоммерческими и коммерческими организациями, физическими лицами: правила эксплуатации и ограничения применения
- 4. Информационные войны

Технология

- В широком смысле это объем знаний, которые можно использовать для производства товаров, работ, услуг.
- В узком смысле способ преобразования вещества, энергии, информации в процессе изготовления продукции, контроля качества, управления.

Информационная технология

- совокупность методов, производственных и программно-технических средств, объединенных в технологическую цепочку, обеспечивающую сбор, хранение, обработку, вывод и распространение информации.
- Информационные технологии предназначены для снижения трудоемкости процессов использования информационных ресурсов.

ИТ

- процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (ст. 2 ФЗ «Об информации, ИТ и о защите информации»).

Таким образом, ИТ это

- а) процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации
- б) способы поиска, сбора, хранения, обработки, предоставления, распространения информации, то есть область применения.

Виды ИТ:

- 1. Высокие интеллектуальные ИТ – генерация технических решений, реализующих ситуационное моделирование, позволяющее выявить связь элементов и их динамику и обозначить объективные закономерности среды (математические формулы, алгоритмы)
- Высокая технология - совокупность информации, знаний, опыта, материальных средств при разработке, создании и производстве новой продукции и процессов в любой отрасли экономики, имеющих характеристики высшего мирового уровня.

Виды ИТ

- 2. Вспомогательные ИТ – ориентированы на обеспечение выполнения определенных функций (1С-бухгалтерия, 1С-предприятия – ведение системы кадров, статистики, система стратегического управления юридическим лицом и др.).

Виды ИТ

- Коммуникационные ИТ – обеспечивают развитие телекоммуникации и ее систем (технологии общения, в т.ч. средства связи – сотовая связь, электросвязь и т.п., программы для ЭВМ- электронная почта, скайп и др.)

Электросвязь

- любые излучение, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам (ст. 2 ФЗ «О связи»).
- При этом под средствами связи понимаются технические и программные средства, используемые для формирования, приема, обработки, хранения, передачи, доставки сообщений электросвязи или почтовых отправлений, а также иные технические и программные средства, используемые при оказании услуг связи или обеспечении функционирования сетей связи.

Правовые основы:

- Конституция РФ
- ФЗ «О связи»
- ГК РФ
- ФЗ «Об информации, ИТ и о защите информации»
- и др.

Основные направления гос. регулирования в сфере ИТ:

- 1. регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (отношения по информатизации);

Основные направления гос. регулирования в сфере ИТ:

- 2. развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

Основные направления гос. регулирования в сфере ИТ:

- 3. создание условий для эффективного использования в РФ информационно-телекоммуникационных сетей, в том числе сети "Интернет" и иных подобных сетей.

Гос. органы, органы м/с в соответствии со своими полномочиями:

- участвуют в разработке и реализации целевых программ по информатизации;
- создают информационные системы и обеспечивают доступ к содержащимся в них ИР на русском языке и государственном языке соответствующей республики в составе РФ.

Порядок создания ИТ

- В соответствии с ч. 1 ст. 44 Конституции РФ каждому гарантируется свобода литературного, художественного, научного, технического и других видов творчества. Интеллектуальная собственность охраняется законом.
- В соответствии с п. "о" ст. 71 Конституции РФ к исключительному ведению Российской Федерации отнесено правовое регулирование интеллектуальной собственности.

Основания для создания ИТ

- Собственная инициатива
- Производственная обязанность в рамках трудовых отношений
- обязательство по договору на выполнение научно-исследовательских, опытно-конструкторских и технологических работ (глава 38 ГК РФ)

Формы представления ИТ

- научное описание или математическое представление программы для ЭВМ,
- в виде микросхемы (изделия)
- в форме комплекта программ для определенной информационной системы и др.

Программы для ЭВМ

- представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.

Программа для ЭВМ

- являются результатами интеллектуальной деятельности, которым предоставляется правовая охрана (то есть признаются интеллектуальной собственностью).

Программа для ЭВМ

- Согласно статье 1261 ГК РФ авторские права на все виды программ для ЭВМ (в том числе на операционные системы и программные комплексы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код, охраняются так же, как авторские права на произведения литературы.

Гос. регистрация программ для ЭВМ

- может осуществляться по желанию обладателя исключительного авторского права.
- Исключение составляет запрет государственной регистрации программ для ЭВМ, баз данных и топологий интегральных микросхем, содержащих сведения, составляющие государственную тайну (п. 1 ст. 1262, п. 1 ст. 1452) и некот. др..

Государственная регистрация программ для ЭВМ

- (внесение соответствующих сведений в государственный реестр и выдача охранного документа) указанных объектов интеллектуальной собственности предоставляет правообладателю ряд несомненных преимуществ в доказывании своих прав на эти объекты.

Концепция использования ИТ в деятельности федерал. органов гос. власти до 2010 года

- приоритетами в использовании ИТ органами государственной власти являются повышение эффективности:
- межведомственного взаимодействия;
- предоставления государственных услуг населению и организациям;
- персональной и коллективной работы сотрудников федеральных органов государственной власти.

- В Доктрине информационной безопасности 2000 года ИТ включены в качестве 3-ей составляющей национальных интересов РФ в информационной сфере.

Введенные ограничения на свободное создание и применение ИТ в области

- разработки программ, нарушающих нормальное функционирование информационных и телекоммуникационных систем (создание помех, глушителей)
- 2. внедрение в апробированные программы изделий и компонентов, реализующих функции не предусмотренных документацией на эти программы (вирусы)

Введены ограничения на свободное создание и применение ИТ в области

- компрометация (раскрытие) ключей и средств криптографической защиты (шифрование) – хакерство
- 4. воздействие на параллельно ключевые системы защиты автоматизированных систем обработки и передачи информации (хакерство и воздействие в форме вирусов).
- 5. внедрение электронных устройств для перехвата информации в технических устройствах обработки, хранения и передачи информации (подслушивающее устройство)

Информационная война

- это действия для достижения информационного превосходства, для поддержки национальной военной стратегии посредством воздействия на информацию и информационные системы противника при одновременном обеспечении безопасности и защиты собственной информации.

Особенности информационной войны:

- охватывает в качестве самостоятельных объектов воздействия все виды информации и информационных систем
- информация может выступать и как оружие, и как объект защиты
- территория и производство ведения войны осуществляется на неограниченном пространстве
- информационная война ведется как при объявлении войны, так и в кризисных ситуациях в различных сферах жизнедеятельности
- ведется как военными, так и гражданскими структурами (избирательный пиар)

Концепция информационной войны

- Подавление (в военное время) элементов инфраструктуры государственного и военного управления (поражение центров командования и управления)
- Радиоэлектронная борьба (электромагнитное воздействие в виде помех и т.д на элементы информационных и телекоммуникационных систем.)

Концепция ведения информационной войны

- Радиоэлектронная разведка
- «Хакерная» война или несанкционированный доступ к информационным ресурсам с последующим их искажением, уничтожением либо хищением или нарушением нормального функционирования этих систем
- Психологические операции или формирование и массовое распространение по информационным каналам противника или глобальным сетям дезинформации или тенденциозной информации для воздействия на оценки, намерения и ориентацию населения и лиц, принимающих решения (психологическая война)
- Получение интересующей информации путем перехвата и обработки открытой информации.

Информационное оружие

- это средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспреещения к ним законных пользователей, дезорганизация работы технических средств, вывода из строя телекоммуникационных сетей, компьютерных систем, всех средств высокотехнологичного обеспечения жизни общества и государства.

- По оценкам Совета Безопасности РФ, с появлением новых информационных технологий информационная безопасность как составляющая национальной безопасности вышла на первый план.

Отличие информационного оружия:

- скрытность, то есть возможность достигать целей без видимой подготовки и объявления войны
- масштабность, то есть возможность наносить невосполнимый ущерб без привычного ограничения пространства.

Отличие информационного оружия:

- универсальность, то есть возможность неоднократного использования как военными, так и гражданскими структурами.
- результативность (сопоставимо с оружием массового поражения) – поражает мозг человека, создавая личность с заданными параметрами (тип сознания, искусственные потребности и т.д.), выводит из строя системы управления государства-противника и его вооруженных сил.

военную, экономическую, банковскую, социальную и иные

- дезорганизации деятельности органов государственного управления, местного самоуправления, средств коммуникации, транспорта
- блокирование деятельности отдельных организаций (например, банков), а также базовых отраслей промышленности путем нарушения, например, системы взаиморасчетов, проведения валютно-финансовых махинаций и т.д.

Сфера применения ИО в целях

- массового распространения и внедрения в сознание людей определенных представлений, привычек, стереотипов поведения
- вызова недовольства или паники среди населения
- инициирование крупных техногенных катастроф в результате нарушения штатного управления технологическими процессами и объектами и т.д.

Виды ИО по области применения:

- 1) военного (например, радиолокационное подавление средств связи помехами, силовое воздействие импульсом высокого напряжения через сеть питания, средства генерации естественной речи конкретного человека и др.) и
- 2) невоенного назначения («программные закладки»: речи в речи, изображения на изображении, 25 кадр).

Виды ИО по объектам поражения

- средства поражения компьютерных систем
- средства поражения психики людей.

Организация защиты от ИО

- преодоление отставания в ИТ, так как перед технологически отстающими странами остро стоит проблема защиты собственных информационных ресурсов.
- сохранение качества информации (своевременности, точности, полноты и доступности), в том числе, обеспечение бесперебойного функционирования баз и банков данных

Организация защиты от ИО

- информационная контрразведка, т.е. выявление технических устройств и программ, представляющих опасность для функционирования информационных систем, предотвращение перехвата информации по техническим каналам.
- разработка психологических, культурных и концептуальных установок, образующих систему защитных фильтров от дезорганизации общественного и индивидуального сознания, в том числе, определение механизма воздействия «программных закладок» на психику человека в целях разработки защитных механизмов (создание эстетических фильтров)

Организация защиты от ИО

- защита информации от несанкционированного доступа, искажения или уничтожения, в том числе, подготовка к возможному нанесению массированного удара по мировому кибернетическому пространству (разработка средств защиты систем государственного и военного управления, связи, электроснабжения, службы по чрезвычайным ситуациям).

Практические мероприятия программного характера по защите от ИО

- организация мониторинга и прогнозирования потребностей экономических и иных структур в различных видах информационного обмена через международные сети, организация международного сотрудничества
- разработка государственной программы совершенствования информационных технологий, обеспечивающих подключение национальных сетей к мировому киберпространству при соблюдении требований безопасности информационных ресурсов

продолжение

- установление перечня информации, не подлежащей передаче по открытым сетям
- активное участие в разработке как национального, так и международного законодательства по вопросам обеспечения мировых открытых сетей

Способы защиты информации несанкционированного доступа в ПК

- программные средства защиты информации, в том числе, криптозащита (т.е. шифрование информации с помощью ее искажения). Восстановить сообщение можно только с помощью алгоритма и кода дешифрования.
- меры организационно-административного характера (управление доступом к информации, регистрация и учет пользователей, то есть разработка и принятие правил информационной безопасности на конкретном предприятии) и технического характера (установление антивирусной программы).