Лекции по дисциплине Организационное и правовое обеспечение информационной безопасности

Для 4-го курса Института кибернетики направления Информационная безопасность

Лектор:
ст. преподаватель кафедры КИБ
Шорана Март-ооловна Донгак

Москва, 2018 г.

ЛЕКЦИЯ №1

ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПРАВИЛ ЗАЩИТЫ ИНФОРМАЦИИ

Цель занятия: рассмотреть и проанализировать вопросы ответственности за нарушение правил защиты информации ограниченного распространения конфиденциального характера.

ВВЕДЕНИЕ

ВОПРОС 1. Правовые основы технической защиты информации конфиденциального характера.

ВОПРОС 2. Виды информации ограниченного распространения конфиденциального характера.

ВОПРОС 3. Охрана информации ограниченного распространения конфиденциального характера.

ВОПРОС 4. Характеристика правовых и нормативных документов по защите персональных данных.

ВОПРОС 5. Ответственность за нарушения в информационной сфере.

Введение

ЗАЩИТА ИНФОРМАЦИИ ПРЕДСТАВЛЯЕТ СОБОЙ ПРИНЯТИЕ ПРАВОВЫХ, ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР направленных на:

— обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

— соблюдение конфиденциальности информации ограниченного доступа;

— реализацию права на доступ к информации.

Федеральный закон «Об информации, информационных технологиях и о защите информации», ст. 2.

- **Анализ правового обеспечения**

- Правовое обеспечение планируемых мероприятий в области защиты информации, всегда должно предшествовать принятию решения о реализации любого мероприятия

- **Реализация организационно-правовых мероприятий защиты**

- Комплексное изучение законов и других нормативных актов в области защиты информации является обязательным элементом информационной культуры работающего в этой области специалиста

- **Реализация технических мероприятий по защите информации**

- При реализации технических мероприятий необходимо выполнять требования законодательства Российской Федерации и нормативных правовых документов по лицензированию исполнителей работ, использованию сертифицированных средств защиты, а также обеспечить действующие ограничения на применение специальных технических средств

Структура нормативно-правового обеспечения информационной безопасности

Нормативно-правовое обеспечение информационной безопасности Российской Федерации

- **Нормативно-правовое обеспечение воплощение в жизнь прав и свобод человека и гражданина, реализуемых в информационной сфере**
- **Нормативно-правовое обеспечение интересов Российской Федерации в области развития российской инфраструктуры и эффективного использования отечественных информационных ресурсов**
- **Нормативно-правовое обеспечение безопасности информационных и телекоммуникационных систем, сетей связи и информационных ресурсов**

Основные направления правового обеспечения защиты информации

1. Права собственности, владения и распоряжения информацией
2. Степень открытости информации
3. Порядок отнесения информации к категории ограниченного доступа
4. Организация работ по защите информации
5. Государственное лицензирование деятельности в области защиты информации
6. Порядок создания специальных служб
7. Права и ответственность должностных лиц за защиту информации

КОНСТИТУЦИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Статья 23

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

Статья 24

1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

2. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

КОНСТИТУЦИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Статья 29

4. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом.

5. Гарантируется свобода массовой информации. Цензура запрещается.

Статья 71

В ведении Российской Федерации находятся:

и) федеральные энергетические системы, ядерная энергетика, расщепляющиеся материалы; федеральные транспорт, пути сообщения, информация и связь; деятельность в космосе.

ЗАКОНОДАТЕЛЬНАЯ БАЗА ЗАЩИТЫ ИНФОРМАЦИИ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА

1. Федеральный закон № 149-ФЗ, 2006 «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон № 152-ФЗ, 2006 «О персональных данных».

3. Федеральный закон № 98-ФЗ, 2004 «О коммерческой тайне».

4. Указ Президента Российской Федерации от 6 марта 1997года № 188 «Об утверждении перечня сведений конфиденциального характера».

ЗАКОНОДАТЕЛЬНАЯ БАЗА ЗАЩИТЫ ИНФОРМАЦИИ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА

5. Постановление Правительства РФ от 21 ноября 2011 г. N 957 «Об организации лицензирования отдельных видов деятельности» С изменениями и дополнениями от: 16 апреля, 28 августа, 4, 14 сентября 2012 г.

6. Постановление Правительства РФ от 3 февраля 2012 г. N 79"О лицензировании деятельности по технической защите конфиденциальной информации"

7. Постановление Правительства РФ от 15 августа 2006г. № 532«О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»

Основные положения Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Регулированию подлежат отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;
2) применении информационных технологий;
3) обеспечении защиты информации.

Основные ПРИНЦИПЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ отношений в сфере информации, информационных технологий и защиты информации:

- установление ограничений доступа к информации только федеральными законами;
- обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
- достоверность информации и своевременность ее предоставления;

Информация

- **Общедоступная информация**
- **Информация ограниченного доступа - доступ к которой ограничен федеральными законам**

Обладатель информации при осуществлении своих прав обязан:

- принимать меры по защите информации;
- ограничивать доступ к информации, если такая обязанность установлена федеральными законам

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен Федеральными законами

ФЕДЕРАЛЬНЫЙ ЗАКОН от 27 июля 2006 № 149-ФЗ
«Об информации, информационных технологиях и о защите информации»

С т а т ь я 2. Основные понятия, используемые в ФЗ

1. Информация – сведения (сообщения, данные) независимо от формы их представления.

5. Обладатель информации – лицо, самостоятельно создавшее информацию, либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким либо признакам.

7. Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

ФЕДЕРАЛЬНЫЙ ЗАКОН от 27 июля 2006 № 149-ФЗ
«Об информации, информационных технологиях и о защите информации»

С т а т ь я 9. Ограничение доступа к информации

4. Федеральными Законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

5. Информация, полученная гражданами (физическими лицами) при исполнении ими определенных видов деятельности (профессиональная тайна) подлежит защите в случаях, если на эти лица ФЗ возложены обязанности по соблюдению конфиденциальности такой информации.

ФЕДЕРАЛЬНЫЙ ЗАКОН от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

С т а т ь я 16. Защита информации

1.Защита информации, представляет собой принятие правовых, организационных и технических мер, направленных на:

-обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

-соблюдение конфиденциальности информации ограниченного доступа;

- реализацию права на доступ к информации

Основные положения Федерального закона «Об информации, информационных технологиях и о защите информации»

- Обязательность соблюдения конфиденциальности информации, доступ к которой ограничен федеральными законами (ст. 9.2);

- Обязательность ввода государственной информационной системы в эксплуатацию в порядке, установленном заказчиком (ст. 14.5);

- Методы и способы защиты информации при создании и эксплуатации государственных информационных систем должны соответствовать требованиям, установленным ФОИВ, уполномоченным в области ПДТР и ТЗИ (ст.16.5)

- Установленные Федеральным законом от 27.07.2006 № 149-ФЗ требования к государственным информационным системам, распространяются на муниципальные информационные системы, если иное не предусмотрено законодательством Российской Федерации (ст.13.4).

Основные положения Федерального закона «Об информации, информационных технологиях и о защите информации»

Обязанности обладателя информации, оператора информационной системы *(ст.16.4)*:

- **предотвращение несанкционированного доступа к информации, не имеющим права на доступ к информации;**
- **своевременное обнаружение фактов несанкционированного доступа к информации;**
- **предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;**
- **недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;**
- **возможность незамедлительного восстановления информации, модифицированной или уничтоженной в следствие несанкционированного доступа к ней;**
- **постоянный контроль за обеспечением уровня защищенности информации.**

ВОПРОС 1.
ПРАВОВЫЕ ОСНОВЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА

СИСТЕМА — комплекс, состоящий из процессов, технических и программных средств, устройств и персонала, обладающий возможностью удовлетворять установленным потребностям или целям.

Государственный стандарт Российской Федерации
ГОСТ Р ИСО/МЭК 12207-99.
Информационная технология.
Процессы жизненного цикла программных средств

ГОСТ Р ИСО/МЭК 12207-99 применяется при приобретении систем, программных продуктов и оказании соответствующих услуг; а также при поставке, разработке, эксплуатации и сопровождении программных продуктов и программных компонентов программно-аппаратных средств как в самой организации, так и вне ее.

СИСТЕМА — специфическое воплощение информационной технологии с конкретным назначением и условиями эксплуатации (ГОСТ Р ИСО/МЭК 15408-1-2008, ст.2.51).

Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 15408-1-2008 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель"

(утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 519-ст)

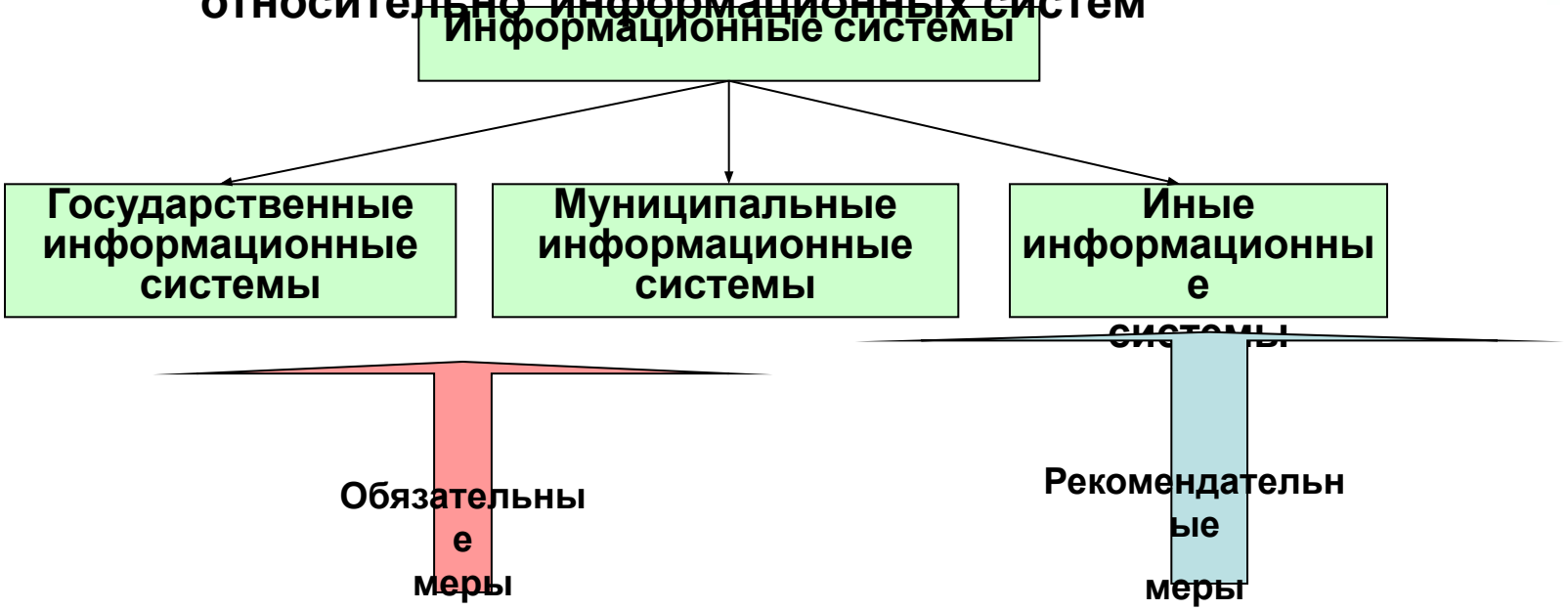
ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ — приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных.

Межгосударственный стандарт ГОСТ 34.003-90.
Информационная технология.
Комплекс стандартов на автоматизированные системы.
Автоматизированные системы.
Термины и определения.

ЗАЩИЩАЕМАЯ ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ – информационная технология, предназначенная для сбора, хранения, обработки, передачи и использования защищаемой информации с требуемым уровнем ее защищенности.

Р 50.1.053-2005
Рекомендации по стандартизации. Информационные технологии. Основные термины и определения в области технической защиты информации.

Основные положения Федерального закона «Об информации, информационных технологиях и о защите информации» относительно информационных систем



Особенности подключения государственных информационных систем к ИТКС (Интернет) могут быть установлены нормативным правовым актом Президента Российской Федерации

Требования по защите информации установленные ФСТЭК России

Порядок создания и эксплуатации ИС, не являющихся государственными или муниципальными, определяется операторами таких ИС в соответствии с требованиями законодательства Российской Федерации

ФЕДЕРАЛЬНЫЙ ЗАКОН
«Об информации, информационных технологиях и о защите информации»

С т а т ь я 5. Информация как объект правовых отношений

1. Информация может являться объектом публичных, гражданских и иных правовых отношений.

Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

ФЕДЕРАЛЬНЫЙ ЗАКОН
«Об информации, информационных технологиях и о защите информации»

С т а т ь я 6. Обладатель информации

1. Обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.

5. Обладатель информации, если иное не предусмотрено федеральными законами вправе:

1) Разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
2) Использовать информацию, в том числе распространять ее по своему усмотрению;
3) Передавать информацию другим лицам по договору или на ином установленном законом основании;
4) Защищать установленным законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

Статья 17. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации

1. Нарушения требований … влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа, вправе обратиться за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные ФЗ требования о защите информации.

ВОПРОС 2.

Виды информации ограниченного распространения конфиденциального характера

Указ Президента Российской Федерации от 6 марта 1997 г. № 188

ПЕРЕЧЕНЬ
сведений конфиденциального характера

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2. Сведения, составляющие тайну следствия и судопроизводства.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской федерации и федеральными законами (служебная тайна).

4. **Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и так далее).**

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской федерации и федеральными законами (коммерческая тайна).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Информация с ограниченным доступом

ПЕРСОНАЛЬНЫЕ ДАННЫЕ — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (Федеральный закон «О персональных данных», ст. 3).

(*сведения, ставшие известными работнику органа записи актов гражданского состояния в связи с государственной регистрацией акта гражданского состояния, являются персональными данными)*

ПРОФЕССИОНАЛЬНАЯ ТАЙНА (ПТ) — информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности. Объекты ПТ: врачебная тайна, тайна связи, тайна переписки, телефонных переговоров, иных сообщений, нотариальная тайна, адвокатская тайна, тайна усыновления, тайна страхования, тайна исповеди. ФЗ от 27.07 2006 № 149. К ПТ не относится коммерческая и государственная.

СЛУЖЕБНАЯ ТАЙНА — защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения

КОММЕРЧЕСКАЯ ТАЙНА — режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду («О коммерческой тайне» от 29.07.2004 № 98-ФЗ);

ВОПРОС 3.
Охрана информации ограниченного распространения конфиденциального характера

Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ

(последняя редакция)

Федеральный закон «О коммерческой тайне»

Статья 3

п.1. КОММЕРЧЕСКАЯ ТАЙНА - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

(п. 1 в ред. Федерального закона от 18.12.2006 N 231-ФЗ).

п.2. ИНФОРМАЦИЯ, СОСТАВЛЯЮЩАЯ КОММЕРЧЕСКУЮ ТАЙНУ (СЕКРЕТ ПРОИЗВОДСТВА), - сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании
и в отношении которых обладателем таких сведений введен режим коммерческой тайны;

(п. 2 в ред. Федерального закона от 18.12.2006 N 231-ФЗ)

Федеральный закон «О коммерческой тайне»

Статья 4.

ПРАВО НА ОТНЕСЕНИЕ ИНФОРМАЦИИ К ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ, И СПОСОБЫ ПОЛУЧЕНИЯ ТАКОЙ ИНФОРМАЦИИ

1. Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации с учетом положений настоящего Федерального закона.
2. Утратил силу с 1 января 2008 года. - Федеральный закон от 18.12.2006 N 231-ФЗ.
3. Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом.
4. Информация, составляющая коммерческую тайну, обладателем которой является другое лицо, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации, составляющей коммерческую тайну, мер по охране конфиденциальности этой информации, а также если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, обладателем которой является другое лицо, и что осуществляющее передачу этой информации лицо не имеет на передачу этой информации законного основания.

Федеральный закон «О коммерческой тайне»

Статья 5. СВЕДЕНИЯ, КОТОРЫЕ НЕ МОГУТ СОСТАВЛЯТЬ КОММЕРЧЕСКУЮ ТАЙНУ

Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;
2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;
3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;
4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

Федеральный закон «О коммерческой тайне»

5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

Федеральный закон «О коммерческой тайне»

Статья 10. ОХРАНА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ (КИ)

п.1. Меры по охране КИ, принимаемые ее обладателем, должны включать:

1) определение перечня информации, составляющей коммерческую тайну;

2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

Федеральный закон «О коммерческой тайне»

4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5) нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна" с указанием обладателя этой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

п.2. Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер, указанных в части 1 настоящей статьи.

Федеральный закон «О коммерческой тайне»

Статья 11. ОХРАНА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В РАМКАХ ТРУДОВЫХ ОТНОШЕНИЙ

п.1. В целях охраны конфиденциальности информации работодатель обязан:

1) ознакомить под расписку работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты;
2) ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;
3) создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

п.2. Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями.

Федеральный закон «О коммерческой тайне»

Статья 13. ОХРАНА КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ ПРИ ЕЕ ПРЕДОСТАВЛЕНИИ

1. Органы государственной власти, иные государственные органы, органы местного самоуправления в соответствии с настоящим Федеральным законом и иными федеральными законами обязаны создать условия, обеспечивающие охрану конфиденциальности информации, предоставленной им юридическими лицами или индивидуальными предпринимателями.

2. Должностные лица органов государственной власти, иных государственных органов, органов местного самоуправления, государственные или муниципальные служащие указанных органов без согласия обладателя информации, составляющей коммерческую тайну, не вправе разглашать или передавать другим лицам, органам государственной власти, иным государственным органам, органам местного самоуправления ставшую известной им в силу выполнения должностных (служебных) обязанностей информацию, составляющую коммерческую тайну, за исключением случаев, предусмотренных настоящим Федеральным законом, а также не вправе использовать эту информацию в корыстных или иных личных целях.

3. В случае нарушения конфиденциальности информации должностными лицами органов государственной власти, иных государственных органов, органов местного самоуправления, государственными и муниципальными служащими указанных органов эти лица несут ответственность в соответствии с законодательством Российской Федерации.

ВОПРОС 4.

Характеристика правовых и нормативных документов по защите персональных данных

Основные положения Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»

Федеральным законом регулируются отношения, связанные с обработкой персональных данных

Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением случаев, обезличивания персональных данных и в отношении общедоступных персональных данных

Федеральными законами могут быть установлены особенности учета персональных данных в государственных и муниципальных информационных системах персональных данных, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей государственной или муниципальной информационной системе персональных данных, конкретному субъекту персональных данных.

Меры по обеспечению безопасности персональных данных при их обработке

Оператор обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных.

ФСТЭК России осуществляет контроль выполнения требований обеспечения безопасности

Требования к обеспечению безопасности персональных данных установлены Постановлением Правительства Российской Федерации от 17.11.2007 №781

Нормативные документы в области защиты персональных данных

Федеральный Закон «О персональных данных»

Регулирует отношения, связанные с обработкой персональных данных с использованием средств автоматизации

Постановление Правительства РФ от 1 ноября 2012 г. N 1119
"Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

Устанавливает требования к обеспечению безопасности персональных данных при их обработке в ИСПДн

«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»

Определяется из показателей исходной защищенности, к которым относятся: 1. Территолриальное размещение системы, наличие подключений к Интернет, разграничение доступа к ПД (всего -7): первый – исходная защищенность системы;

2. Частота (вероятность реализации угрозы, которая определяется экспертным образом.

Базовые модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

(Приказ ФСТЭК России от 18 февраля 2013 г. N 21)

Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (Приказ ФСТЭК России от 11 февраля 2013 г. N 17)

Приказ ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г.

№ 55/86/20

Порядок проведения классификации информационных систем персональных данных.

Определение перечня актуальных угроз, согласно базовой модели.

Определяет порядок проведения классификации информационных систем персональных данных

Определяет методы и способы обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных

Постановление Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

Настоящий документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных и уровни защищенности таких данных.

Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы.

Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом АКТУАЛЬНЫХ УГРОЗ безопасности персональных данных и информационных технологий, используемых в информационных системах.

Постановление Правительства РФ от 1 ноября 2012 г. N 1119

"Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные (далее — оператор), или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора (далее — уполномоченное лицо).

Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

Постановление Правительства РФ от 1 ноября 2012 г. N 1119

"Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

Согласно п.6 данного Положения Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, СВЯЗАННЫЕ с наличием недокументированных (недекларированных) возможностей в СИСТЕМНОМ программном обеспечении, используемом в

Информационная система персональных данных

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, СВЯЗАННЫЕ с наличием недокументированных (недекларированных) возможностей в ПРИКЛАДНОМ программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, НЕ СВЯЗАННЫЕ с наличием недокументированных (недекларированных) возможностей в СИСТЕМНОМ и ПРИКЛАДНОМ программном обеспечении, используемом в информационной системе.

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают:

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- учет лиц, допущенных к работе с персональными данными в информационной системе;

- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
описание системы защиты персональных данных.

Методические документы ФСТЭК России в области обеспечения безопасности персональных данных, при их обработке в ИСПД

Методические документы ФСТЭК России

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

Методические документы предназначены для использования при проведении работ по обеспечению безопасности персональных данных при их обработке в следующих информационных системах персональных данных:

- **ИСПД государственных органов;**
- **ИСПД муниципальных органов;**
- **ИСПД юридических лиц;**
- **ИСПД физических лиц.**

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Базовая модель угроз предназначена для решения следующих задач:

разработки частных моделей угроз безопасности персональных данных в конкретных информационных системах с учетом их назначения, условий и особенностей функционирования;

анализа защищенности информационных систем персональных данных от угроз безопасности в ходе организации и выполнения работ по обеспечению безопасности персональных данных;

разработки системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем персональных данных;

проведения мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

недопущения воздействия на технические средства информационных систем персональных данных, в результате которого может быть нарушено их функционирование;

контроля за обеспечением уровня защищенности персональных данных.

Базовая модель угроз безопасности персональных данных содержит:

Классификация угроз безопасности персональных данных.

Анализ и характеристики угроз возможной утечки по техническим каналам.

Анализ и характеристики угроз несанкционированного доступа к информации в информационной системе персональных данных, включая характеристики источников угроз несанкционированного доступа, характеристики уязвимостей системного и прикладного программного обеспечения, характеристики угроз безопасности персональных данных, реализуемых с использованием протоколов межсетевого взаимодействия и программно-математических воздействий, характеристики нетрадиционных информационных каналов и результатов несанкционированного или случайного доступа.

Типовые модели угроз безопасности персональных данных, обрабатываемых в информационных системах (автоматизированных рабочих местах, локальных и распределенных информационных системах) не имеющих и имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Методика определения актуальных угроз безопасности предназначена для формирования перечня актуальных угроз безопасности персональным данным, обрабатываемым в информационных системах.

- **Формирование перечня источников угроз персональным данным осуществляется методом экспертного опроса. На основе экспертного опроса и анализа результатов сетевого сканирования информационной системы формируется перечень ее уязвимых звеньев. По данным обследования информационной системы формируется перечень возможных технических каналов утечки информации.**
- **Путем анализа указанных перечней определяются условия существования в информационной системе угроз безопасности информации и составляется их полный перечень.**
- **На основании полного перечня угроз безопасности информации в соответствии с порядком определения актуальных угроз безопасности персональных данных в информационных системах персональных данных формируется перечень актуальных угроз безопасности персональным данным.**

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

На стадии ввода информационных систем в эксплуатацию осуществляется оценка соответствия информационной системы требованиям безопасности

Оценка соответствия информационных систем персональных данных требованиям безопасности информации проводится:

для информационных систем 1 и 2 классов – сертификация (аттестация) по требованиям безопасности информации;

для информационных систем 3 класса – декларирование соответствия или сертификация (аттестация) по требованиям безопасности информации (по решению оператора);

для информационных систем 4 класса оценка соответствия проводится по решению оператора.

В соответствии с положениями Федерального закона «О лицензировании отдельных видов деятельности» и требованиями постановления Правительства Российской Федерации «О лицензировании деятельности по технической защите конфиденциальной информации» операторы информационных систем персональных данных при проведении мероприятий по обеспечению безопасности персональных данных (конфиденциальной информации) при их обработке в информационных системах 1, 2 классов и распределенных информационных систем 3 класса должны получить лицензию на осуществление деятельности по технической защите

РУКОВОДЯЩИЕ ДОКУМЕНТЫ ФСТЭК ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

РД «РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» 1992 г.

РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» 1992 г.

РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» 1997 г.

РД «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники» 1992 г.

РД «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» 2001 г.

РД «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» 2002 г.

СПЕЦИАЛЬНЫЕ ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ (СТР-К)

СТРУКТУРА ДОКУМЕНТА

- Термины, определения и сокращения
- Общие положения
- Организация работ по защите конфиденциальной информации
- Требования и рекомендации по защите речевой конфиденциальной информации
- Требования и рекомендации по защите конфиденциальной информации, обрабатываемой в автоматизированных системах
- Рекомендации по обеспечению защиты конфиденциальной информации, содержащейся в негосударственных информационных ресурсах, при взаимодействии абонентов с информационными сетями общего пользования
- Приложения

ПРИЛОЖЕНИЯ К СТР-К

Основные нормативные правовые акты и методические документы по защите информации.

Пример документального оформления перечня сведений конфиденциального характера

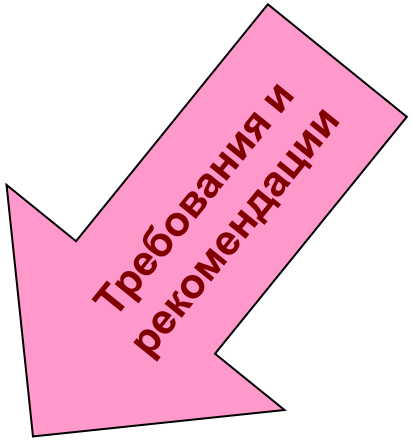
Форма технического паспорта на автоматизированную систему

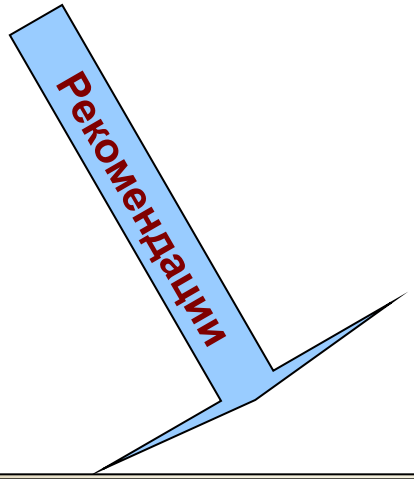
Форма технического паспорта на защищаемое помещение

Форма аттестата соответствия автоматизированной системы

Форма аттестата соответствия защищаемого помещения Форма акта классификации автоматизированной системы,предназначенной для обработки конфиденциальной информации

СТР-К





По защите государственных информационных ресурсов некриптографическим и методами

По защите негосударственных информационных ресурсов, составляющих коммерческую тайну, банковскую тайну

«Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К)

Защите подлежат:

Информационные ресурсы информационных систем

Совокупность файлов данных, составляющих информацию пользователей и программных продуктов, определяющих информационную технологию.

Средства и системы информатизации

СВТ, АС различного уровня и назначения на базе СВТ, в т. ч. информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных, технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), средства защиты информации, используемые для защиты конфиденциальной информации

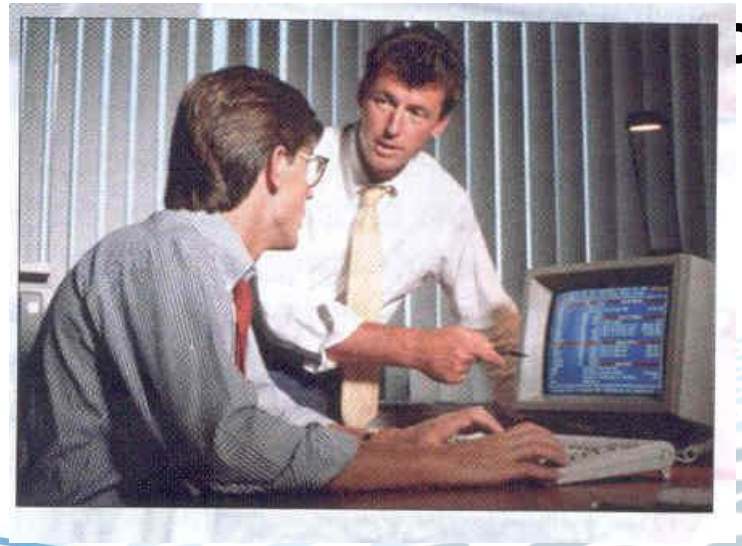
Технические средства и системы,

Не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается (циркулирует);

Помещения

для ведения переговоров со сведениями ограниченного доступа

Защите подлежит речевая информация и информация, обрабатываемая техническими средствами, а также представленная в виде информативных электрических сигналов, физических полей, носителей на бумажной, о-оптической и иной основе.



ОСНОВНЫЕ ПОЛОЖЕНИЯ «СПЕЦИАЛЬНЫХ ТРЕБОВАНИЙ И РЕКОМЕНДАЦИЙ» ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

1. Защита информации на объекте информатизации достигается выполнением комплекса организационных мероприятий и применением (при необходимости) средств защиты информации от утечки информации или воздействия на нее по техническим каналам, за счет несанкционированного доступа к ней, по предупреждению преднамеренных программно-технических воздействий с целью нарушения целостности (модификации, уничтожения) информации в процессе ее обработки, передачи и хранения, нарушения ее доступности и работоспособности технических средств.

2. Ответственность за обеспечение требований по технической защите конфиденциальной информации возлагается на руководителей организаций, эксплуатирующих объекты информатизации.

3. Разработка мер и обеспечение защиты информации осуществляются подразделениями по защите информации или отдельными специалистами, назначаемыми руководителями организаций для проведения таких работ. Разработка мер защиты информации может осуществляться также сторонними организациями, имеющими лицензии ФСТЭК России.

4. Для защиты конфиденциальной информации используются сертифицированные по требованиям безопасности информации технические средства защиты информации.

Государственные стандарты

ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России

ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. Госстандарт России

ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России

ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России

ГОСТ Р ИСО 7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. Госстандарт России

ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Госстандарт России

ГОСТ Р ИСО/МЭК 15408-1-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Ведение и общая модель. Госстандарт России

ГОСТ Р ИСО/МЭК 15408-2-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России

ГОСТ Р ИСО/МЭК 15408-3-2008. Методы и средства обеспечения

Система
нормативных и методических документов по безопасности ИТ

	1 уровень	2 уровень	3 уровень	4 уровень
1 группа	Технический регламент О безопасности ИТ	Концепция обеспечения безопасности изделий ИТ	Положение по обеспечению безопасности в жизненном цикле	Типовая программа обеспечения безопасности изделий ИТ Базовая модель обеспечения безопасности в жизненном цикле ИТ
2 группа	Разработка завершена в2005 Технический регламент О требованиях к средствам обеспечения безопасности ИТ	ГОСТ ИСО/МЭК 15408-2008. «ИТ. Методы и средства ОБ. Критерии оценки безопасности ИТ» Введен с 1.01.2004г.	Руководящий документ (2002г.) Критерии оценки безопасности ИТ Положение по разработке ПЗ и ЗБ Профили защиты Руководство по регистрации профилей защиты	Общая методология оценки безопасности изделий ИТ Базовая модель угроз безопасности изделий ИТ Руководство по формированию семейств ПЗ Руководство по разработке ПЗ и ЗБ
3 группа		Положение о порядке оценки соответствия ….	Требования к участникам системы оценки соответствия Положение по инспекционному контролю за деятельностью испытательных лабораторий	Руководство для испытательной лаборатории Руководство для органов сертификации Руководство для заявителя

ДОКУМЕНТЫ ПЕРВОГО УРОВНЯ (Программа разработки технических регламентов на 2005-2006 годы, утверждена Правительством Российской Федерации от 6.11.2004 г. №1421-р)

Включают технические регламенты:

«О безопасности информационных технологий»

«О требованиях к средствам обеспечения безопасности информационных технологий.

Определяют:

Основные понятия в области ИТ;

Перечень объектов технического регулирования, для которых риск реализации угроз может быть недопустимо велик;

Виды потенциальных угроз безопасности ИТ и способы их реализации;

Порядок анализа и оценки рисков угроз безопасности ИТ;

Категории объектов технического регулирования в зависимости от риска реализации угроз;

Требования безопасности для каждой категории объектов технического регулирования;

Порядок проведения контроля и надзора.

ДОКУМЕНТЫ ПЕРВОГО УРОВНЯ

(Программа разработки технических регламентов на 2005-2006 годы)

ПРОГРАММА РАЗРАБОТКИ ТЕХНИЧЕСКИХ РЕГЛАМЕНТОВ

(утв. распоряжением Правительства Российской Федерации от 6 ноября 2004 г. № 1421-р)

(с изменениями от 8 ноября 2005 г., 1 февраля, 29 мая 2006 г., 28 декабря 2007 г., 25 сентября, 10 декабря 2008 г., 1 апреля, 20 августа 2009 г.)

(в редакции распоряжения Правительства Российской Федерации от 9 марта 2010 г. № 300-р).

ДОКУМЕНТЫ ВТОРОГО УРОВНЯ

Включают:

1. «Концепция обеспечения безопасности изделий информационных технологий» (2005г)

Основные понятия и общие положения по безопасности изделий ИТ.

Назначение, структура и основное содержание документов по безопасности изделий ИТ (профиля защиты и задания по безопасности).

Основные меры безопасности при разработке и эксплуатации изделий ИТ.

2. «ГОСТ Р ИСО/МЭК 15408-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». (Введен с 1 октября 2009 г.)

Содержит функциональные требования к средствам ИТ и требования доверия.

3. Постановления Правительства Российской Федерации и положения «О стандартизации оборонной продукции» и «О порядке оценки соответствия оборонной продукции и продукции, используемой в целях ЗИ ограниченного доступа» (Срок разработки проектов 2005г.)

ДОКУМЕНТЫ ТРЕТЬЕГО УРОВНЯ

Конкретизируют требования документов второго уровня:

1. Положение по обеспечения безопасности при разработке , испытаниях, поставке и эксплуатации изделий информационных технологий»

Система положений по достижению требуемого уровня безопасности ИТ;

Общие требования по безопасности на различных этапах изделий ИТ

2. РД « Безопасность информационных технологий. Критерии оценки безопасности информационных технологий». Соответствует ГОСТ Р ИСО ИСО/ МЭК 15408-2008 и предназначен для заказчиков, разработчиков, пользователей изделий ИТ, органов по оценке соответствия с обеспечением оперативного внесения изменений по опыту практического применения.

3. «Положение по разработке профилей защиты и заданий по безопасности»

Определяет порядок разработки , оценки, регистрации и публикации профилей защиты и заданий по безопасности для изделий ИТ, предназначенных для обработки информации ограниченного доступа.

4. «Руководство по регистрации профилей защиты»

Профиль защиты – НД со стандартизированным набором требований по безопасности изделий ИТ

5.«Положение по инспекционному контролю за деятельностью участников системы оценки соответствия»

Определяет порядок и процедуры контроля за соблюдением

ДОКУМЕНТЫ ЧЕТВЕРТОГО УРОВНЯ

Определяют методы и способы достижения требований, задаваемых в документах первых трех уровней.

1. «Базовая модель обеспечения безопасности в жизненном цикле ИТ»
2. «Типовая программа обеспечения безопасности при разработке и сопровождении изделия ИТ»
   Определяют соответствующие этапу меры и работы по обеспечению безопасности с учетом принятой модели жизненного цикла средства ИТ
3. «Общая методология оценки безопасности изделий ИТ»
   Содержит совокупность типовых методик оценки выполнения требований безопасности ИТ.
4. «Базовая модель угроз безопасности изделий ИТ.
   Устанавливает структуру модели угроз, форму представления угроз в профилях защиты и заданиях по безопасности, описание типовых угроз для изделий ИТ.
5. «Руководство по формированию семейств профилей защиты»
   Устанавливает порядок формирования семейств профилей защиты, состав классов защищенности изделий ИТ и соответствующих им базовых пакетов требований доверия и уровней стойкости функций безопасности.
6. «Руководство по разработке профилей защиты и заданий по безопасности»
   Методический документ к РД «Безопасность ИТ. Критерии оценки безопасности ИТ.
7. Руководства для участников системы оценки соответствия.
   Определяют основные процедурные и методические аспекты деятельности участников системы оценки соответствия, их задачи и порядок взаимодействия

ГОСТ Р ИСО/МЭК 17799-2005

"Информационные технологии. Методы безопасности. Руководство по управлению безопасностью информации"

Первая часть «Практические рекомендации»

Определяет и рассматривает следующие аспекты информационной безопасности:

- **ПОЛИТИКА БЕЗОПАСНОСТИ;**
- **организация защиты;**
- **классификация и управление информационными ресурсами;**
- **управление персоналом;**
- **физическая безопасность;**
- **администрирование компьютерных систем и сетей;**
- **управление доступом к системам;**
- **разработка и сопровождение систем;**
- **планирование бесперебойной работы организации;**
- **проверка системы на соответствие требованиям информационной безопасности.**

Вторая часть «Спецификации системы» - рассматривает аспекты информационной безопасности с точки зрения сертификации информационной системы на соответствие требованиям стандарта.

ГОСТ Р ИСО/МЭК 17799-2005

"Информационные технологии. Методы безопасности. Руководство по управлению безопасностью информации"

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель: обеспечение решения вопросов информационной безопасности и вовлечение высшего руководства организации в данный процесс.

Разработка и реализация политики информационной безопасности организации осуществляется высшим руководством путем выработки четкой позиции в решении вопросов информационной безопасности.

Документальное оформление

Политика информационной безопасности должна быть утверждена, издана и надлежащим образом доведена до сведения всех сотрудников организации. Она должна устанавливать ответственность руководства, а также излагать подход организации к управлению информационной безопасностью.

Примерная структура типовой политики безопасности организации и перечень инструкций в соответствии с ГОСТ Р ИСО/МЭК 17799-2005

ПРИМЕРНАЯ СТРУКТУРА ТИПОВОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ

- 1. Общие положения.
  - 1.1. Назначение документа.
  - 1.2. Основания для разработки документа.
  - 1.3. Основные определения.
- 2. Идентификация системы.
  - 2.1. Идентификатор и имя системы.
  - 2.2. Ответственные подразделения.
  - 2.3. Режим функционирования системы.
  - 2.4. Описание и цели системы.
  - 2.5. Цели и задачи политики безопасности.
  - 2.6. Системная среда.
  - 2.6.1. Физическая организация системы.
  - 2.6.2. Логическая организация системы.
  - 2.7. Реализованные сервисы системы.
  - 2.8. Общие правила, принятые в системе.
  - 2.9. Общее описание важности информации.
- 3. Средства управления.
  - 3.1. Оценка рисков и управление.
  - 3.2. Экспертиза системы защиты информации.
  - 3.3. Правила поведения, должностные обязанности и ответственность.
- 4. Функциональные средства.
  - 4.1. Защита персонала.
  - 4.2. Управление работой и вводом-выводом.
  - 4.3. Планирование непрерывной работы.
  - 4.4. Средства поддержки программных приложений.
  - 4.5. Средства обеспечения целостности информации.
  - 4.6. Документирование.
  - 4.7. Осведомленность и обучение специалистов.
  - 4.8. Ответные действия в случаях возникновения происшествий.
- 5. Технические средства.
  - 5.1. Требования к процедурам идентификации и аутентификации.
  - 5.2. Требования к системам контроля и разграничения доступа.
  - 5.3. Требования к системам регистрации сетевых событий.

Примерная структура типовой политики безопасности организации и перечень инструкций в соответствии с ГОСТ Р ИСО/МЭК 17799-2005

ПРИМЕРНАЯ СТРУКТУРА ТИПОВОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ

Примерные инструкции по реализации политики безопасности

1. Требования к защите портов и служб.
2. Порядок проведения экспертизы системы защиты информации.
3. Порядок проведения анализа рисков.
4. Использование автоматизированных систем анализа защищенности.
5. Порядок восстановления автоматизированных систем после аварийных ситуаций.

Основные положения стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0–2008)

Стандарт устанавливает:

- общие и специальные принципы безопасного функционирования организации банковской системы;
- модели угроз и нарушителей информационной безопасности организаций банковской системы Российской Федерации;
- состав и назначение политики информационной безопасности организаций банковской системы Российской Федерации;
- общие (основные) требования по обеспечению информационной безопасности, отображаемые в политиках информационной безопасности организации;
- управление информационной безопасностью организации банковской системы Российской Федерации;
- модель зрелости процессов управления информационной безопасностью организаций банковской системы Российской Федерации;
- аудит и мониторинг информационной безопасности организаций банковской системы Российской Федерации;
- направления дальнейшего развития стандарта

ВОПРОС 5.

Ответственность за нарушения в информационной сфере

ОСНОВНЫЕ НАКАЗУЕМЫЕ ДЕЯНИЯ В ИНФОРМАЦИОННОЙ СФЕРЕ

КОДЕКС

Российской Федерации об административных правонарушениях от 30.12.2001 №195-ФЗ

Глава 13. Административные правонарушения в области связи и информации

Статья 13.12. Нарушение правил защиты информации

п. 2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), влечет наложение административного штрафа на должностных лиц – от 10 до 20 МРОТ, на юридических лиц – от 100 до 200 МРОТ.

п. 4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, - влечет наложение административного штрафа на должностных лиц – от 30 до 40 МРОТ, на юридических лиц – от 200 до 300 МРОТ.

ТРУДОВОЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

Статья 90. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

- Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

ТРУДОВОЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

ОСНОВАНИЯ И ПРОЦЕДУРА УВОЛЬНЕНИЯ ЗА РАЗГЛАШЕНИЕ КОММЕРЧЕСКОЙ ТАЙНЫ

Статьей 81 Трудового кодекса Российской Федерации предусмотрено такое основание для расторжения трудового договора, как разглашение охраняемой законом тайны:

- государственной,
- коммерческой,
- служебной
- иной, ставшей известной работнику в связи с исполнением им трудовых обязанностей.

ТРУДОВОЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИМЕР:

В пункте 43 постановления Пленума Верховного Суда Российской Федерации № 2 "О применении судами Российской Федерации Трудового кодекса Российской Федерации" сказано, что в случае оспаривания работником увольнения по подпункту "в" пункта 6 статьи 81 Трудового кодекса Российской Федерации работодатель ОБЯЗАН ПРЕДОСТАВИТЬ ДОКАЗАТЕЛЬСТВА, свидетельствующие о том, что:

- СВЕДЕНИЯ, КОТОРЫЕ РАБОТНИК РАЗГЛАСИЛ, ОТНОСЯТСЯ К ОХРАНЯЕМОЙ ЗАКОНОМ ТАЙНЕ;

- ОНИ СТАЛИ ИЗВЕСТНЫ РАБОТНИКУ В СВЯЗИ С ИСПОЛНЕНИЕМ ИМ ТРУДОВЫХ ОБЯЗАННОСТЕЙ;

- СОТРУДНИК ОРГАНИЗАЦИИ ОБЯЗЫВАЛСЯ НЕ РАЗГЛАШАТЬ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ.

ТРУДОВОЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

ВЫВОД:

Если ваш работник разгласил служебную или коммерческую тайну, то с него в обязательном порядке должно быть затребовано письменное объяснение; а при отказе его дать, необходимо составить соответствующий акт.

ОТКАЗ РАБОТНИКА ОТ ДАЧИ ПИСЬМЕННЫХ ОБЪЯСНЕНИЙ НЕ ЯВЛЯЕТСЯ ПРЕПЯТСТВИЕМ ДЛЯ НАЛОЖЕНИЯ ДИСЦИПЛИНАРНОГО ВЗЫСКАНИЯ.

ТРУДОВОЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

Следует учитывать, что согласно трудовому законодательству, дисциплинарное взыскание можно наложить на работника не позднее одного месяца со дня обнаружения его проступка, не считая времени болезни работника или пребывания его в отпуске.

Оно не может быть применено позднее 6 месяцев со дня совершения проступка, а по результатам ревизии или проверки финансово-хозяйственной деятельности - не позднее двух лет со дня его совершения.

ТРУДОВОЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

МАТЕРИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОММЕРЧЕСКОЙ ТАЙНЫ

Статья 243 ТК РФ устанавливает полную материальную ответственность работника за разглашение сведений, составляющих служебную, коммерческую или иную охраняемую законом тайну в случаях, предусмотренных федеральным законом.

Материальная ответственность работника может иметь место при наличии следующих обязательных элементов состава правонарушения:

ТРУДОВОЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

Материальная ответственность работника может иметь место при наличии следующих обязательных элементов состава правонарушения:

- прямого действительного ущерба;
- противоправного поведения работника;
- причинной связи между действиями (бездействиями) работника и причиненным ущербом;
- вины работника в причиненном ущербе.

ТРУДОВОЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

Говоря о наступлении материальной ответственности работника, стоит обратить внимание на следующее противоречие законодательства.

ПО ОБЩЕМУ ПРАВИЛУ, МАТЕРИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ РАБОТНИКА ОГРАНИЧЕНА ЕГО СРЕДНЕМЕСЯЧНЫМ ЗАРАБОТКОМ.

В ряде случаев, в том числе когда происходит разглашение охраняемой законом тайны, работник может нести полную материальную ответственность.

Это значит, что правомерным будет "удержать" не одну, а две, три, четыре и т.д. его заработные платы, но лишь для возмещения прямого действительного ущерба!

Неполученные доходы (упущенная выгода) взысканию с работника не подлежат согласно статье 238 ТК РФ.

УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

В январе 1997 г. вступил в силу Уголовный кодекс Российской Федерации (УК РФ), в соответствии с которым в нашей стране криминализированы (т.е. признаны уголовно наказуемыми) определенные деяния в сфере компьютерной информации, несущие повышенную общественную опасность.

В частности, нормы о преступлениях в означенной сфере зафиксированы в трех статьях УК РФ:

— ст. 272 (Неправомерный доступ к компьютерной информации),

— ст. 273 (Создание, использование и распространение вредоносных программ для ЭВМ)

— ст. 274 (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей)

УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

Общим объектом названных преступлений являются общественные отношения в сфере обеспечения информационной безопасности, а к непосредственным объектам преступного посягательства относятся базы и банки данных конкретных компьютерных систем или сетей, их отдельные файлы, а также компьютерные технологии и программные средства их обеспечения, включая средства защиты компьютерной информации.

УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

Согласно ст. 272 УК РФ, уголовная ответственность за неправомерный доступ к компьютерной информации наступает, если это деяние повлекло за собой хотя бы одно из следующих негативных последствий:

а) уничтожение, блокирование, модификацию либо копирование информации;

б) нарушение работы ЭВМ или их сети.

УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

СТАТЬЯ 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

СТАТЬЯ 272. Неправомерный доступ к компьютерной информации

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, -

наказывается

— штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет,

— либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов,

— либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев,

— либо лишением свободы на срок до пяти лет.

УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

В отличие от описанной нормы ответственность по ч.1 ст. 273 УК РФ предусматривается вне зависимости от наступления общественно опасных последствий. Она предусмотрена за сам факт совершения одного из следующих действий:

а) создание программы для ЭВМ или внесение изменений в существующие программы, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети;

б) использование либо распространение таких программ или машинных носителей с такими программами.

УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

СТАТЬЯ 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами -

наказываются

— лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, -

наказываются лишением свободы на срок от трех до семи лет.

УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

Огромный вред наносят нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Это может не только привести к сбоям в работе оборудования, но в некоторых случаях и полностью парализовать работу предприятия, учреждения или организации.

УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

Поэтому законодательно установлено, что в случае причинения существенного вреда в результате указанных действий, а также при наступлении по неосторожности тяжких последствий описанные деяния наказуемы в уголовном порядке, если они повлекли уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ (ст. 274 УК РФ).

УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, -

наказывается

— штрафом в размере до 500 000 рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев,

— либо исправительными работами на срок от шести месяцев до одного года,

— либо ограничением свободы на срок до двух лет,

— либо принудительными работами на срок до двух лет,

— либо лишением свободы на тот же срок.

УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, -

наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

В случае противоправного использования возможностей компьютерной техники и современных средств связи уже сейчас достаточно трудно юридически верно определить место совершения преступления.

С учетом существующих технических возможностей и тенденций развития преступного мира можно прогнозировать осложнение ситуации.

Представляется, что место расположения ЭВМ, с помощью которой злоумышленник совершает посягательство, крайне редко будет совпадать с местом расположения объекта посягательства.

УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

Кроме того, для уголовно-правовой квалификации деяний иногда значимо место, где наступили вредные последствия общественно опасного деяния.

Если объектом посягательства явилась компьютерная информация, то преступные последствия деяния, в свою очередь, могут наступить в месте, отличном от места хранения этой информации.

С учетом возможностей, предоставляемых компьютерными сетями, нельзя исключить, что преступные последствия наступят либо в какой-то конкретной и единственной точке земного шара, либо на территории нескольких государств, либо на территории всех государств, имеющих доступ в сеть.

СПАСИБО
ЗА ВНИМАНИЕ