	До	После
Знания о материале		
Полезность материала		

Нормативная правовая база обеспечения информационной безопасности и технической защиты информации в таможенных органах Российской Федерации

Лекция

Учебные вопросы

1. Нормативная правовая база обеспечения информационной безопасности и технической защиты информации в таможенных органах РФ.
2. Ответственность за нарушения установленных требований по обеспечению информационной безопасности.
3. Направления совершенствования информационной безопасности таможенных органов Российской Федерации.

1. Нормативная правовая база обеспечения информационной безопасности и технической защиты информации в таможенных органах РФ

К **правовым** методам обеспечения информационной безопасности РФ относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности РФ. При этом, наиболее важными направлениями этой деятельности являются:

1. Внесение изменений и дополнений в законодательство РФ, регулирующее отношения в области обеспечения информационной безопасности, в целях:

- создания и совершенствования системы обеспечения информационной безопасности РФ;
- устранения внутренних противоречий в федеральном законодательстве;
- устранения противоречий, связанных с международными соглашениями, к которым присоединилась;
- конкретизации правовых норм, устанавливающих ответственность за правонарушения в области обеспечения информационной безопасности РФ.

2. Законодательное разграничение полномочий в области обеспечения информационной безопасности РФ между органами государственной власти.

3. Определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан.

4. Разработка и принятие нормативных правовых актов, устанавливающих ответственность юридических и физических лиц за нарушения информационной безопасности.

5. Законодательное закрепление приоритета развития национальной информационной инфраструктуры и др.

Правовая база в сфере информационной безопасности Федеральной таможенной службы включает пакет Федеральных законов, Кодексов РФ, Указов Президента РФ, постановлений Правительства РФ и др. нормативных актов, базирующихся на Конституции РФ и международных обязательствах государства, а также нормативные акты ФТС России.


Правила, регламенты, инструкции
Политика информационной безопасности
Нормативно-правовые акты министерств и ведомств, методические документы
Стандарты РФ (ГОСТ Р)
Международные стандарты
Постановления правительства РФ
Федеральные законы, кодексы РФ, Указы Президента РФ, доктрины и концепции
Конституция РФ
Международные нормы и обязательства

Основные правовые нормативные акты по обеспечению информационной безопасности на государственном уровне

1. Доктрина информационной безопасности Российской Федерации от 09.09.2000.
2. Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 04 июня 1996 г. № 85-ФЗ «Об участии в международном информационном обмене».
4. Закон Российской Федерации от 21 июля 1993 г.№ 5485-I «О государственной тайне».
5. Федеральный закон от 29.07.2004 № 98-ФЗ "О коммерческой тайне".
6. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Основные правовые нормативные акты по обеспечению информационной безопасности на государственном уровне

7. НМД Гостехкомиссии России. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К);
8. ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечен ия безопасности. Критерии оценки безопасности информационных технологий»;
9. РД Гостехкомиссии России. АС. Защита от НСД к информации. Классификация АС и требования по защите информации;
10. РД Гостехкомиссии России. СВТ. Защита от НСД к информации. Показатели защищенности информации;
11. РД Гостехкомиссии России. Безопасность информационных технологий. Критерии оценки

Нормативные акты по информационной безопасности ФТС России организационного характера

1. Таможенный кодекс Таможенного союза.
2. Концепция обеспечения информационной безопасности таможенных органов Российской Федерации на период до 2020 года, утверждена Приказом ФТС России от 13 декабря 2010 г. № 2401.
3. Приказ ФТС России от 22 августа 2011 г. N 1702 «Об утверждении Положения и состава Совета по обеспечению информационной безопасности таможенных органов Российской Федерации».
4. Типовое положение о подразделении информационной безопасности и технической защиты информации регионального таможенного управления, утверждено приказом ФТС России от 28 января 2011 г. № 165.

Нормативные акты по информационной безопасности ФТС России организационного характера

5. Положение об отделе информационной безопасности Главного управления информационных технологий, утверждено приказом ФТС России от 20 июля 2007 г. № 885.
6. Положение о должностном лице, ответственном за защиту информации в структурном подразделении ФТС России, утверждено приказом ФТС России от 07 июня 2008 г. № 710.
7. Временное положение об информационных ресурсах таможенных органов, их формировании и использовании (утверждены приказом ГТК России от 15 марта 2004 г. № 315).

Нормативные акты ФТС России по криптозащите и электронной подписи

1. Приказ ФТС России от 28 июня 2012 г. № 1266 «Об утверждении Порядка эксплуатации средств криптографической защиты информации, реализующих механизмы электронной подписи, должностными лицами (работниками) таможенных органов Российской Федерации».
2. Временное руководство администратору безопасности по разграничению доступа к базам данных таможенных органов (утверждено приказом ГТК России от 16 июля 2001 г. № 670).
3. Положение о порядке эксплуатации персональных средств идентификации и аутентификации должностных лиц таможенных органов Российской Федерации (утверждено приказом ФТС России от 15.04.2009 № 683).

Нормативные акты ФТС России по криптозащите и электронной подписи

4. Приказ ФСБ РФ от 09.02.2005 № 66 (ред. от 12.04.2010) "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)".
5. Положение о Доменной структуре ЕСК ЕАИС ТО (утверждено приказом ФТС России от 12 октября 2010 г. № 779).
6. Порядок предоставления должностным лицам таможенных органов доступа к ресурсам центральной базы данных ЕАИС таможенных органов (утвержден приказом ФТС России от 02 февраля 2007 г. № 168).
7. Приказ ФСБ РФ от 27.12.2011 № 795 "Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи".
8. Требования по обеспечению информационной безопасности при работе с ресурсами Центральной базы данных ЕАИС таможенных органов (утверждены приказом ФТС России от 12 ноября 2007 г. № 1393).

Нормативные акты ФТС России по организационным мерам защиты информации

1. Временное руководство администратору безопасности по разграничению доступа к базам данных таможенных органов (утверждено приказом ГТК России от 16 июля 2001 г. № 670).
2. Порядок предоставления должностным лицам таможенных органов доступа к ресурсам центральной базы данных ЕАИС таможенных органов (утвержден приказом ФТС России от 2 февраля 2007 г. № 168).
3. Требования по обеспечению информационной безопасности при работе с ресурсами Центральной базы данных ЕАИС таможенных органов (утверждены приказом ФТС России от 12 ноября 2007 г. № 1393).
4. Типовое положение о подразделении информационной безопасности и ТЗИ регионального таможенного управления, типовое положение подразделения информационной безопасности и технической защиты информации таможни (утверждены приказом ФТС России от 28 января 2011 г. № 165).

Нормативные акты ФТС России по техническим мерам защиты информации

1. Положение об Автоматизированной системе выявления каналов утечки информации из Центральной базы данных ЕАИС таможенных органов (утверждено приказом ФТС России от 22 января 2008 г. № 39).
2. Порядок предоставления технической документации, регламентирующей взаимодействие информационных систем таможенных органов и информационных систем, предназначенных для представления участниками внешнеэкономической деятельности сведений таможенным органам в электронной форме (приказ ФТС России от 24 января 2008 № 52).

Нормативные акты ФТС России по техническим мерам защиты информации

1. Временный порядок по использованию ведомственной электронной почты для передачи между таможенными органами электронных копий документов, содержащих сведения ограниченного распространения, и не содержащих сведений, составляющих государственную тайну (распоряжение ФТС России от 27.08.2007 г. № 282-р).
2. Типовые требования по безопасности информации, предъявляемые к программным средствам информационных систем и информационных технологий таможенных органов (Приложение № 1 к Порядку организации процессов жизненного цикла программных средств информационных систем и информационных технологий таможенных органов, утвержденным приказом ФТС России от 3 февраля 2010 г. № 183).

2. Ответственность за нарушения установленных требований по обеспечению информационной безопасности.

КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ ОБ АДМИНИСТРАТИВНЫХ ПРАВОНАРУШЕНИЯХ (КоАП РФ) от 30.12.2001 N 195-ФЗ (принят ГД ФС РФ 20.12.2001)

- **Глава 13. Административные правонарушения в области связи и информации**
- Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)
-
- Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) -
- влечет предупреждение или наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц - от пятисот до одной тысячи рублей; на юридических лиц - от пяти тысяч до десяти тысяч рублей.

Трудовой кодекс РФ (ТК РФ) от 30.12.2001 N 197-ФЗ

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, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном настоящим Кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ (УК РФ)
от 13.06.1996 N 63-ФЗ
(принят ГД ФС РФ 24.05.1996)
(действующая редакция)

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 исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ (УК РФ)
от 13.06.1996 N 63-ФЗ
(принят ГД ФС РФ 24.05.1996)
(действующая редакция)

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 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.

2. Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

a. 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, – наказывается лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

b. Те же деяния, повлекшие по неосторожности тяжкие последствия, – наказываются лишением свободы на срок от трех до семи лет.

3. Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

a. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, – наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

b. То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок до четырех лет.

3. Направления совершенствования информационной безопасности таможенных органов Российской Федерации

http://www.an.ru/techno/article/43911

Жизнь под присмотром: как за нами следят с помощью «маяков», «жучков» и «топтунов»

Автор: Георгий Александров

Хотите, чтобы никто не знал, где вы, — не носите с собой ноутбуки и КПК, прочие коммуникаторы и спутниковые навигаторы.

Многие из них даже в выключенном (!) состоянии способны не только выдать ваше местоположение, но и записывать разговоры и незаметно для хозяина отсылать их в виде архивированных файлов. Популярные трубки с так называемым тачскрином и мощным процессором вообще дают возможность оператору и спецслужбам получать доступ ко всей заложенной в них информации — записной книжке, фото, видео и т. д.