Тема доклада: Нормативное регулирование в области информационной безопасности и защиты персональных данных на предприятиях

Язов Юрий Константинович

Главный научный сотрудник

ГНИИИ ПТЗИ ФСТЭК России

доктор технических наук, профессор

Тлф. раб.(473)261-97-12 (раб.)

(473)234-79-79 (деж.)

(8)903-651-42-69 (моб.)

Факс (473)253-15-35

Email:gniii@fstec.ru

Система документов по ТЗИ, не составляющей государственную тайну (ГТ)

Основные законы в области ТЗИ

Федеральный закон Российской Федерации от 27 июля 2006 г. №149-ФЗ: Об информации, информационных технологиях и о защите информации.

Федеральный закон Российской Федерации от 27 июля 2006 г. №152-ФЗ : О персональных данных.

Федеральный закон Российской Федерации от 25 июля 2011 г. №261-ФЗ "О внесении изменений в Федеральный закон "О персональных данных"

Российская Федерация. Федеральный закон от 29 июля 2004 г. № 98-ФЗ: О коммерческой тайне.

Основные документы по терминологии в области ТЗИ

ГОСТ Р 50922 – 2006. «Защита информации. Основные термины и определения».

ГОСТ Р 53114 - 2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

Унифицированный глоссарий союзного государства в области информационной безопасности. 2002 г.

Законы Российской Федерации, специальные нормативные документы

Аспекты организации ТЗИ, регулируемые нормативными и методическими документами

Порядок и общие требования по организации ТЗИ (технологии проведения работ по ТЗИ) на объектах информатизации

- **Оценка обстановки: категорирование объектов информатизации и информационных ресурсов**
- **Оценка обстановки: выявление и оценка опасности угроз безопасности информации, оценка защищенности информации**
- **Обоснование требований по ТЗИ**
- **Обоснование требований к средствам и системе ТЗИ**
- **Выбор способов и средств ТЗИ, построение систем защиты информации**
- **Аттестация средств и систем защиты**
- **Контроль ТЗИ**
  - Организация контроля
  - Оценка возможностей и эффективности контроля
  - Обоснование требований к средствам и системам контроля
  - Выбор способов и средств контроля, построение систем

Нормативные документы, регламентирующие требования по ТЗИ

СТР-К

Приказ Гостехкомиссии России от 2.03.2001 №282

РД «АС. Защита от НСД к информации. Классификация АС и требования по ЗИ»

Гостехкомиссия России 1992 г.

РД «СВТ. Защита от НСД к информации. Показатели защищенности.

Гостехкомиссия России 1992 г.

Методические рекомендации по технической защите информации, составляющей коммерческую тайну.

ФСТЭК России 25 декабря 2006 г.

ГОСТ Р 52633 (0 - 5) – 2006 – 2010 гг. Требования к средствам высоконадежной биометрической аутентификации

РД. Защита от НСД к информации. Часть 1. ПО средств ЗИ. Классификация по уровню контроля отсутствия НДВ. М.; 1999 г.

РД. СВТ. Межсетевые экраны. Защита от НСД к информации Показатели защищенности от НСД к информации. М.: 1997.

Основные документы, определяющие технологию проведения работ по защите персональных данных

Специальные требования и рекомендации по защите конфиденциальной информации (СТР-К). Приказ председателя Гостехкомиссии России от 2.03.2001 г.

Порядок проведения классификации информационных систем персональных данных, утвержденный приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20

Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных. Постановление Правительства РФ от 17.11.2007 г. №781

Положение о методах и способах защиты информации в информационных системах персональных данных. Приказ директора ФСТЭК России от 5 февраля 2010 г. №58.

Категорирование объектов информатизации

Классы защищенности информации в АС в соответствии с РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»

Третья группа

В АС работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности.

- 3Б
- 3А

Вторая группа

В АС пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности

- 2Б
- 2А

Первая группа

В многопользовательской АС одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС

- 1Д
- 1Г
- 1В
- 1Б
- 1А

Категорирование объектов информатизации

Классы защиты информации в СВТ в соответствии с РД «Средства вычислительной техники. Защиты от несанкционированного доступа к информации. Показатели защищенности. Гостехкомиссия России 1992 г.

Категорирование объектов информатизации

По важности

Классы информационные системы персональных данных

- ИСПДн 1 класса (К1), для которых нарушение безопасности ПДн может привести к значительным негативным последствиям для субъектов персональных данных
- ИСПДн 2 класса (К2), для которых нарушение безопасности ПДн может привести к негативным последствиям для субъектов персональных данных
- ИСПДн 3 класса (К3), для которых нарушение безопасности ПДн может привести к незначительным негативным последствиям для субъектов персональных данных
- ИСПДн 4 класса (К4), для которых нарушение безопасности ПДн не приводит к негативным последствиям для субъектов персональных данных

Классификация ИСПДн проводится оператором в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20

Основные документы, регламентирующие процедуры анализа угроз

Рассмотренные ранее документы, определяющие технологию проведения работ по ТЗИ, а также:

ГОСТ Р 51275-2006. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

Базовая модель угроз безопасности персональных данных при обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15.02.2008

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 14.032.2008

Федеральный закон Российской Федерации от 25 июля 2011 г. №261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», Статья 19, п.2

Обеспечение безопасности Пдн достигается:

1) **определением угроз безопасности** Пдн при их обработке в ИСПдн;

2) применением организационных и технических мер по обеспечению безопасности Пдн при их обработке в ИСПдн, необходимых для выполнения требований к защите Пдн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности Пдн;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) **оценкой эффективности принимаемых мер** по обеспечению безопасности Пдн до ввода в эксплуатацию ИСПдн;

5) учетом машинных носителей Пдн;

6) **обнаружением фактов несанкционированного доступа** к Пдн и принятием мер;

7) восстановлением Пдн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к Пдн, обрабатываемым в ИСПдн, а также обеспечением регистрации и учета всех действий, совершаемых с Пдн в ИСПдн;

9) **контролем** за принимаемыми мерами по обеспечению безопасности Пдн и уровня защищенности ИСПдн.