ЭЛВИС-ПЛЮС

ОПЫТ РАЗРАБОТКИ ДОКУМЕНТАЦИИ СЗПДн. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПДн.

(Требования, комментарии, рекомендации)

ОАО «ЭЛВИС-ПЛЮС»

2009 год

ЭЛВИС-ПЛЮС

Требования к составу документации СЗПДн

Требования к составу документации СЗПДн, разрабатываемой оператором, устанавливаются:

- **Постановлением Правительства РФ от 17.11.2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в ИСПДн».**
- **Документами уполномоченных федеральных органов:**
  - ✔ ФСБ России;
  - ✔ ФСТЭК России.

ЭЛВИС-ПЛЮС

Перечень основной документации СЗПДн

1. Положение по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн.
2. ***Модель угроз безопасности персональных данных***.
3. Акт классификации ИСПДн.
4. Требования по обеспечению безопасности ПДн при их обработке в ИСПДн.
5. Описание системы защиты персональных данных.
6. Перечень применяемых средств защиты информации.
7. Заключение о возможности эксплуатации средств защиты информации (разрабатывается по результатам проверки готовности к использованию СЗИ) (Приёмо-сдаточная документация на СЗИ).
8. Правила пользования средствами защиты информации.
9. Рекомендации (инструкции) по использованию программных и аппаратных средств защиты информации.
10. Список лиц, доступ которых к ПДн, обрабатываемым в ИС, необходим для выполнения служебных (трудовых) обязанностей (утверждается оператором или уполномоченным лицом).
11. Должностные инструкции персоналу в части обеспечения безопасности ПДн при их обработке в ИСПДн.

ЭЛВИС-ПЛЮС

Обязанности операторов
(Постановление Правительства РФ 2007 г. № 781)

Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных (уполномоченное лицо). *(п. 10)*

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

а) определение *угроз безопасности персональных данных* при их обработке, формирование на их основе *модели угроз.* *(п. 12)*

ЭЛВИС-ПЛЮС

Что такое модель угроз?
(основные понятия)

Модель угроз **- систематизированный перечень актуальных угроз безопасности ПДн при их обработке в ИСПДн.**

Угрозы безопасности ПДн - совокупность условий факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий при их обработке в ИСПДн.

Источник угрозы - субъект доступа, территориальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Нарушитель безопасности ПДн - физическое лицо случайно или преднамеренно совершающее действия, следствием которого является нарушение безопасности ПДн при их обработке техническими средствами в ИСПДн.

Уязвимость ИСПДн - недостаток ИСПДн, предоставляющий возможность реализации угроз безоп-ти обрабатываемых в ней ПДн.

ИСПДн - ИС, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и ТС, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таких средств.

ЭЛВИС-ПЛЮС

Зачем нужна модель угроз?

Выявление и учёт угроз безопасности ПДн в конкретных условиях составляет основу для планирования и осуществления мероприятий, направленных на обеспечение безопасности ПДн при их обработке в ИСПДн, в том числе позволяет обеспечить:

- Формирование обоснованных требований по защите ПД при их обработке в ИСПДн.
- Реализацию дифференцированного подхода к обеспечению безопасности ПДн с целью минимизации затрат на защиту ИСПДн.

ЭЛВИС-ПЛЮС

Нормативные документы

1. Базовая модель угроз безопасности ПДн при их обработке в ИСПДн

- **Содержит общее системное изложение вероятных угроз безопасности ПД при их обработке в ИСПДн.**
- **Предназначена для использования при разработке моделей угроз для конкретных ИСПДн.**

2. Методика определения угроз безопасности ПДн при их обработке в ИСПДн

- **Определяет порядок моделирования угроз безопасности ПД при их обработке в ИС и выявления актуальных угроз** (на основе экспертного анализа).
- **Результаты определения актуальных угроз используются для определения конкретных организационно-технических требований по защите ИСПДн и для выбора СЗИ.**

ЭЛВИС-ПЛЮС

Предметная область модели угроз

ЭЛВИС-ПЛЮС

Угрозы безопасности ПДн

- **Угрозы безопасности ПД могут быть реализованы за счёт:**
  - ✓ несанкционированного доступа к базам данных;
  - ✓ утечки ПД по техническим каналам.

Угрозы, связанные с НСД

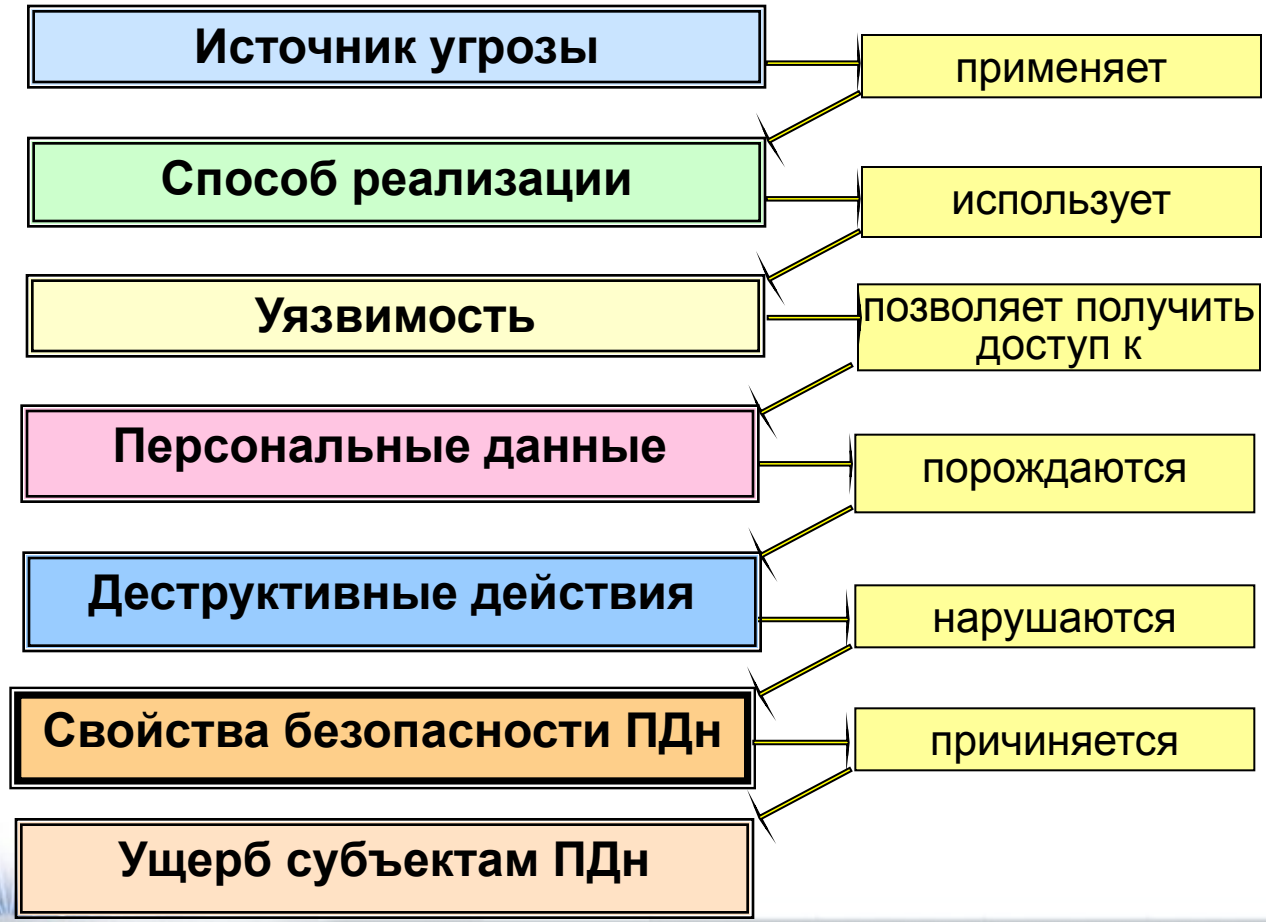
Угрозы, связанные с НСД (угрозы НСД в ИСПДн), представляются в виде совокупности обобщенных классов возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения ИСПДн, способов реализации угроз, объектов воздействия (носителей защищаемой информации) и возможных деструктивных действий.

Угроза НСД описывается следующей формализованной записью:

<источник угрозы>, <уязвимость программного и аппаратного обеспечения>, <способ реализации угрозы>, <объект воздействия (носитель ПДн)>, <несанкционированный доступ>.

ЭЛВИС-ПЛЮС

Логическая взаимосвязь составных элементов угрозы



ЭЛВИС-ПЛЮС

Основные угрозы НСД и возможные последствия их реализации

№ п/п	Тип угрозы	Возможные последствия
1	Анализ сетевого трафика	Исследование характеристик сетевого трафика, *перехват передаваемых данных*, в том числе идентификаторов и паролей пользователей
2	Сканирование сети	Определение протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, активных сетевых сервисов, идентификаторов и паролей пользователей
3	Угроза выявления пароля	Выполнение любого действия, связанного с получением несанкционированного доступа
4	Подмена доверенного объекта сети	Изменение трассы прохождения сообщений, несанкционированное изменение маршрутно-адресных данных. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации
5	Навязывание ложного маршрута сети	Несанкционированное изменение маршрутно-адресных данных, анализ и модификация передаваемых данных, навязывание ложных сообщений
6	Внедрение	Перехват и просмотр трафика. Несанкционированный доступ

№ п/п	Тип угрозы		Возможные последствия
7	Отказ в обслужи-вании	Частичное исчерпание ресурсов	Снижение пропускной способности каналов связи, производительности сетевых устройств. Снижение производительности серверных приложений
		Полное исчерпание ресурсов	Невозможность передачи сообщений из-за отсутствия доступа к среде передачи, отказ в установления соединения. Отказ в предоставлении сервиса (электронной почты, файлового и т.д.)
		Нарушение логической связности между атрибутами, данными, объектами	Невозможность передачи, сообщений из-за отсутствия корректных маршрутно-адресных данных. Невозможность получения услуг ввиду несанкционированной модификации идентификаторов, паролей и т.п.
		Использ-е ошибок в ПО	Нарушение работоспособности сетевых устройств.
8	Удален-ный запуск прило-жений	Путем рассылки файлов, содержащих деструктивный код, вирусное заражение	Нарушение конфиденциальности, целостности, доступности информации
		Путем переполнения буфера серверного приложения	
		Путем использ--я	Скрытое управление системой

ЭЛВИС-ПЛЮС

Угрозы утечки ПДн по техническим каналам

- **угрозы утечки акустической (речевой) информации;**
- **угрозы утечки видовой информации;**
- **угрозы утечки информации по каналам ПЭМИН.**

Угрозы утечки ПДн по техническим каналам однозначно описываются характеристиками источника информации, среды (пути) распространения и приемника информативного сигнала, то есть определяются характеристиками технического канала утечки ПДн и описываются следующим образом:

<источник угрозы (приемник информативного сигнала)>, <среда (путь) распространения информационного сигнала>, <источник (носитель) ПДн>.

ЭЛВИС-ПЛЮС

Порядок моделирование угроз безопасности ПДн (1)

- **Исходные данные для определения актуальных угроз:**

  ✓ перечень источников угроз (***формируется на основе опроса***);

  ✓ перечень уязвимых звеньев ИС (***формируется на основе опроса и/или сетевого сканирования***);

  ✓ перечень технических каналов утечки (***формируется на основе обследования ИС***).

ЭЛВИС-ПЛЮС

Порядок моделирования угроз безопасности ПДн (2)

Определение актуальных угроз безопасности ПД в ИСПДн предусматривает следующие этапы:

- ✔ оценка (на основе опроса и анализа) уровня исходной защищённости ИС ПД (- ***высокий, средний, низкий***); (определение ***коэффициента*** Y_1).
- ✔ экспертная оценка частоты (вероятности) реализации угрозы (***маловероятная, низкая, средняя, высокая***) (определение ***коэффициента*** Y_2).
- ✔ расчёт коэффициента реализуемости угрозы: $Y = Y_1 + Y_2$
- ✔ формирование вербальной интерпретации угрозы по значению Y;
- ✔ экспертная оценка опасности угрозы (***низкая, средняя, высокая***)

ЭЛВИС-ПЛЮС

Порядок моделирования угроз безопасности ПДн (3)

определение актуальных угроз осуществляется ***путём исключения неактуальных угроз по правилам, приведённым в таблице***:

Возможность реализации угрозы (Y)	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

ЭЛВИС-ПЛЮС

Пример оценки актуальности угроз

Источник угрозы	Способ реализации	Уязвимость	Дестр. действие	Исх. защ. (Y1)	Вер. угр. (Y2)	Коэф. реал. (Y)	Коэф. реал. верб.	Опас-ть. угрозы	Актуальность
А 1.1	С 1.2	В 4	Е 3.5	10	0	0,5	средняя	средняя	актуальная
А 1.1	С 1.4.2	В 3	Е 3.3; Е 3.4	10	0	0,5	средняя	средняя	актуальная
А 1.1	С 1.4.2	В 3.2	Е 3.3; Е 3.4	10	0	0,5	средняя	средняя	актуальная
А 1.1	С 1.4; С 1.4.5	В 3.2	Е 3	10	0	0,5	средняя	средняя	актуальная
А 1.1	С 2.4	В 4	Е 3.1 - Е 3.4	10	0	0,5	средняя	высокая	актуальная
А 1.1	С 1.4.3	В 1	Е 3.4	10	2	0,6	средняя	низкая	неактуальная
А 1.2.2; А 1.2.3; А 1.2.7	С 1.4.3	В 1	Е 3.4	10	2	0,6	средняя	низкая	неактуальная
А 1.2.2; А 1.2.3; А 1.2.8	С 1.4.3	В 3	Е 3.4	10	2	0,6	средняя	низкая	неактуальная

ЭЛВИС-ПЛЮС

Рекомендуемая структура модели угроз безопасности ПДн

1. Введение
2. Описание ИСПДн.
   - 2.1. Назначение ИСПДн.
   - 2.2. Общая характеристика ИСПДн.
   - 2.3. Описание технологии обработки ПДн в ИСПДн.
3. Перечень угроз безопасности информации с указанием их актуальности.
4. Описание возможных последствий реализации угроз (для основных угроз).

ЭЛВИС-ПЛЮС

Спасибо за внимание !

124460, МОСКВА, Зеленоград,
Центральный проспект, 11
тел. (495) 777-42-92,
факс (499) 731-24-03
e-mail: mb@elvis.ru
e-mail: rom@elvis.ru
http://www.elvis.ru