Модель угроз безопасности персональных данных при их обработке в информационных системах

Имя: Пушин Алексей Владимирович

Должность: консультант сектора науки и информатизации

Организация: Министерство образования и науки Удмуртской Республики

Законодательная необходимость

- п. 2 ст. 19 Федеральног закона от 27.07.2006 N 152-ФЗ «О персональных данных» **Вносит в перечень мер обеспечения безопасности ПДн.(**
- п. 3 ст. 19 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» **устанавливает уровни защищённости, требования к защите ПДн, требования к материальным носителям** биометрических ПДн и **технологиям хранения** таких данных вне ИСПДн (*Требования и уровни защищённости определены постановлением Правительства РФ от 01.11.2012 г. № 1119).*

Нормативно-методические документы по разработке модели угроз

- **Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных** (утв. Заместителем директора ФСТЭК России 15 февраля 2008 г.) (БМУ)
- **Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных** (утв. Заместителем директора ФСТЭК России 14 февраля 2008 г.) (МОАУ)
- **Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации** (утв. Руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/54 – 144) (МР ФСБ)

Этапы моделирования и определения актуальности угроз безопасности ПДн

1. Определения общего перечня угроз ПДн.
2. Определения уровня исходной защищённости.
3. Расчёт актуальности полученных угроз безопасности ПДн.
4. Определение Модели нарушителя безопасности ПДн.
5. Создание документа «Модель угроз безопасности персональных данных при их обработке в информационной системе».

Показатели исходной защищённости ИСПДн

1. **По территориальному размещению.**
2. **По наличию соединения с сетями общего пользования.**
3. **По встроенным (легальным) операциям с записями баз персональных данных.**
4. **По разграничению доступа к персональным данным.**
5. **По наличию соединений с другими базами ПДн иных ИСПДн.**
6. **По уровню обобщения (обезличивания) ПДн.**
7. **По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки.**

Пример определения уровня исходной защищённости

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению:			
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	+
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);	–	–	+
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	–	+	–
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	–	+	–
локальная ИСПДн, развернутая в пределах одного здания	+	–	–

Пример определения уровня исходной защищённости

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования;	–	–	+
ИСПДн, имеющая одноточечный выход в сеть общего пользования;	–	+	–
ИСПДн, физически отделенная от сети общего пользования	+	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных:			
чтение, поиск;	+	–	–
запись, удаление, сортировка;	–	+	–
модификация, передача	–	–	+

Пример определения уровня исходной защищённости

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
4. По разграничению доступа к персональным данным:			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	-	+	-
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	–	–	+
ИСПДн с открытым доступом	–	–	+
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);	–	–	+
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	+	–	–

Пример определения уровня исходной защищённости

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
6. По уровню обобщения (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+	-	-
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	-	+	-
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	-	-	+

Пример определения уровня исходной защищённости

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, предоставляющая всю базу данных с ПДн;	–	–	+
ИСПДн, предоставляющая часть ПДн;	–	+	–
ИСПДн, не предоставляющая никакой информации.	+	–	–

Пример определения уровня исходной защищённости

	Уровень защищенности		
	Высокий	Средний	Низкий
Количество «+» в колонках	3	3	3
РЕЗУЛЬТАТ	НИЗКИЙ		

- ИСПДн имеет ***высокий*** уровень исходной защищенности, если **не менее 70%** характеристик ИСПДн соответствуют уровню **«высокий».**
- ИСПДн имеет ***средний*** уровень исходной защищенности, если **не выполняются условия по пункту 1 и не менее 70%** характеристик ИСПДн соответствуют уровню не ниже **«средний».**
- ИСПДн имеет ***низкую*** степень исходной защищенности, если **не выполняются условия по пунктам 1 и 2**.

Рассматриваемый перечень угроз

- **Утечка информации по каналу побочных электромагнитных излучений и наводок**
- **Утечка речевой информации**
- **Утечка видовой информации**
- **Перехват паролей (идентификаторов)**
- **Модификация BIOS, перехват управления загрузкой**
- **Несанкционированное копирование, уничтожение ПДн**
- **Модификация СУБД ПДн**
- **Внедрение вредоносных программ**

На основе методических рекомендаций «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. Заместителем директора ФСТЭК России 15.02.2008 г.)

Расчёт возможности реализации угрозы

Где Y_1 – числовой коэффициент на основе степени исходной защищённости

$$Y_1 = \begin{cases} 0, \text{если степень исходной защищённости "Высокая"} \\ 5, \text{если степень исходной защищённости "Средняя"} \\ 10, \text{если степень исходной защищённости "Низкая"} \end{cases}$$

Y_2 – числовой коэффициент на основе вероятностной оценки реализация конкретной угрозы безопасности ПДн для данной ИСПДн.

$$Y_2 = \begin{cases} 0 - \text{для маловероятной угрозы;} \\ 2 - \text{для низкой вероятности угрозы;} \\ 5 - \text{для средней вероятности угрозы;} \\ 10 - \text{для высокой вероятности угрозы.} \end{cases}$$

$$Y = \frac{Y_1 + Y_2}{20}$$

$$\text{Возможность реализации угрозы} = \begin{cases} \text{"Низкая", если } 0 \le Y \le 0.3 \\ \text{"Средняя", если } 0.3 < Y \le 0.6 \\ \text{"Высокая", если } 0.6 < Y \le 0.8 \\ \text{"Очень высокая", если } 0.8 < Y \end{cases}$$

Пример расчета вероятности угрозы

№	Угроза	Исходная защ-сть	Вероятностная оценка	Вер-сть реализации угрозы
1	Утечка информации по каналу побочных электромагнитных излучений и наводок	Низкая	Маловероятно	Середняя
		10	0	0,5
2	Утечка речевой информации	Низкая	Низкая	Середняя
		10	2	0,6
3	Утечка видовой информации	Низкая	Низкая	Середняя
		10	2	0,6
4	**Перехват паролей (идентификаторов)**	**Низкая**	**Высокая**	**Оч.выс.**
		10	**10**	**1**
5	**Модификация BIOS, перехват управления загрузкой**	**Низкая**	**Середняя**	**Высокая**
		10	**5**	**0,75**
6	**Несанкционированное копирование, уничтожение ПДн**	**Низкая**	**Середняя**	**Высокая**
		10	**5**	**0,75**
7	**Модификация СУБД ПДн**	**Низкая**	**Середняя**	**Высокая**
		10	**5**	**0,75**
8	**Внедрение вредоносных программ**	**Низкая**	**Высокая**	**Оч.выс.**
		10	**10**	**1**

Информация, входящая в документ «Модель угроз безопасности ПДн при их обработке в ИСПДн»

- **Описание объекта моделирования (анализируемой ИСПДн) и его характеристик.**
- **Перечни характерных для данной ИСПДн источников угроз безопасности ПДн, уязвимостей компонентов ИСПДн, способов нейтрализации данных угроз и уязвимостей в рамках анализируемой ИСПДн, объектов взаимодействия и последствий реализации вышеуказанных способов.**
- **Оценку ущерба (опасности) для субъектов персональных данных от реализации тех или иных угроз безопасности ПДн.**
- **Анализ рисков реализации вышеуказанных угроз.**
- **Описание модели нарушителя безопасности ПДн.**
- **Выводы относительно класса ИСПДн и криптосредств, обязательных к использованию в ИСПДн.**

Спасибо за внимание !