**4. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПДН**

**Порядок определения актуальных угроз безопасности персональных данных в информационных системах персональных данных**

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн. Подход к составлению перечня актуальных угроз состоит в следующем.

Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИСПДн и частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн

Исходная степень защищенности определяется следующим образом.

1. ИСПДн имеет ***высокий*** уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).

2. ИСПДн имеет ***средний*** уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.

3. ИСПДн имеет ***низкую*** степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент Y1 , а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показателя, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

***маловероятно*** – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

***низкая вероятность*** – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

***средняя вероятность*** - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

***высокая вероятность*** - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y2 , а именно:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением

*Y = (Y1 +Y2 )/ 20*

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

если *0 ≤ Y ≤ 0,3* , то возможность реализации угрозы признается низкой;

если *0,3 < Y ≤ 0,6* , то возможность реализации угрозы признается средней;

если *0,6 < Y ≤ 0,8* , то возможность реализации угрозы признается высокой;

если *Y > 0,8* , то возможность реализации угрозы признается очень высокой.

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИСПДн.

Этот показатель имеет три значения:

низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн.

**4.1. Модель угроз безопасности ПДн, обрабатываемых в ИСПДн «Active Directory»**

**4.1.1. Уровень исходной защищённости ИСПДн**

Документом ФСТЭК России «Методика актуализации угроз ПДн» вводится обобщенный показатель уровня исходной защищенности ИСПДн, зависящий от технических и эксплуатационных характеристик ИСПДн. (коэффициент Y1).

В соответствии с заданными критериями оценки определяется уровень исходной защищенности ИСПДн «Active Directory».

|  |  |  |
| --- | --- | --- |
| Технические и эксплуатационные характеристики ИСПДн | | Уровень защищённости |
| 1. По территориальному размещению | корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации | Средний |
| 2. По наличию соединения с сетями общего пользования | ИСПДн, имеющая многоточечный выход в сеть общего пользования | Низкий |
| 3. По встроенным (легальным) операциям с записями баз персональных данных | чтение, поиск | Высокий |
| 4. По разграничению доступа к персональным данным | ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн | Средний |
| 5. По наличию соединений с другими базами ПДн иных ИСПДн | ИСПДн, в которой используется одна база ПДн, принадлежащая организации-владельцу данной ИСПДн | Высокий |
| 6. По уровню обобщения (обезличивания) ПДн | ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации | Средний |
| 7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки | ИСПДн, не предоставляющая никакой информации | Высокий |

По совокупности полученных результатов уровень исходной защищенности ИСПДн «Active Directory» оценивается как средний, поскольку не менее 70% характеристик ИСПДн (86%) соответствуют уровню «средний» или «высокий».

Согласно «Методики актуализации угроз ПДн» ФСТЭК России, коэффициент исходной защищенности ИСПДн «Active Directory» и Y1=5.