Как обеспечивается безопасность персональных данных в автоматизированных системах.

Во-первых, Федеральным законом регулируется порядок обработки данных (например, запрет использования данных для целей, отличающихся от целей, указанных при сборе данных, запрет объединения баз данных, которые были собраны для разных целей и т.д.)

Но по Федеральному закону всё слишком поверхностно. Для понимания фактических способов защиты персональных данных лучше обратиться к приказу ФСТЭК (ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ) №21.

Согласно этому приказу в состав мер по обеспечению безопасности персональных данных:

* идентификация и аутентификация субъектов доступа и объектов доступа;
* управление доступом субъектов доступа к объектам доступа;
* ограничение программной среды;
* защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
* регистрация событий безопасности;
* антивирусная защита;
* обнаружение (предотвращение) вторжений;
* контроль (анализ) защищенности персональных данных;
* обеспечение целостности информационной системы и персональных данных;
* обеспечение доступности персональных данных;
* защита среды виртуализации;
* защита технических средств;
* защита информационной системы, ее средств, систем связи и передачи данных;

Классификация угроз информационных систем

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Существует 3 типа угроз согласно постановлению правительства РФ № 1119:

Угрозы 1-го типа подразумевают недокументированные (незадекларированные) возможности в СИСТЕМНОМ ПО, используемом в информационной системе.

Угрозы 2-го типа подразумевают недокументированные (незадекларированные) возможности в ПРИКЛАДНОМ ПО, используемом в информационной системе.

Угрозы 3-го типа подразумевают иные угрозы, не связанные с недокументированными возможностями и СИСТЕМНОГО и ПРИКЛАДНОГО ПО, используемого в информационной системе.

Уровни защищенности

Согласно приказу ФСТЭК №21 существует 4 уровня защищенности, где чем меньше уровень- тем выше защищенность. В самом приказе есть большая таблица требований к мерам по обеспечению информационной безопасности для каждого из уровней.

В таблицах ниже слово субъект подразумевает, что он НЕ является сотрудником оператора.

Необходимость обеспечения 1-го уровня защиты при хотя бы одном из условий:

|  |  |
| --- | --- |
| Что обрабатывает информационная система | Угроза |
| Биометрические данные | 1-го типа (системное ПО) |
| Специальные категории ПД более чем 10000 субъектов, не являющихся сотрудниками оператора | 2-го типа (прикладное ПО) |

Необходимость обеспечения 2-го уровня защиты при хотя бы одном из условий:

|  |  |
| --- | --- |
| Что обрабатывает информационная система | Угроза |
| Общедоступные ПД | 1-го типа |
| ПД сотрудников оператора или более 100000 субъектов\* | 2-го типа |
| Биометрические данные | 2-го типа |
| Общедоступные ПД более чем 100000 субъектов\* | 2-го типа |
| Иные категории ПД более 100000 субъектов\* | 2-го типа |
| Специальные категории ПД более 100000 субъектов\* | 3-го типа (иные) |

Необходимость обеспечения 3-го уровня защиты при хотя бы одном из условий:

|  |  |
| --- | --- |
| Что обрабатывает информационная система | Угроза |
| Общедоступные ПД сотрудников или более 100000 субъектов\* | 2-го типа |
| Иные категории ПД сотрудников или более 100000 субъектов\* | 2-го типа |
| Специальные категории ПД сотрудников или более 100000 субъектов\* | 3-го типа |
| Биометрические данные | 3-го типа |
| Иные категории ПД сотрудников или более 100000 субъектов\* | 3-го типа |

Необходимость обеспечения 4-го уровня защиты при хотя бы одном из условий:

|  |  |
| --- | --- |
| Что обрабатывает информационная система | Угроза |
| Общедоступные персональные данные | 3-го типа |
| Иные категории ПД сотрудников или МЕНЕЕ 100000 субъектов\* | 3-го типа |