Приложение № 1
к Требованиям к обеспечению
защиты информации в автоматизированных
системах управления производственными
и технологическими процессами
на критически важных объектах,
потенциально опасных объектах,
а также объектах, представляющих
повышенную опасность для жизни
и здоровья людей и для окружающей
природной среды

ОПРЕДЕЛЕНИЕ
КЛАССА ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ

1. Класс защищенности автоматизированной системы управления (первый класс (К1), второй класс (К2), третий класс (К3)) определяется в зависимости от уровня значимости (критичности) обрабатываемой в ней информации (УЗ).

2. Уровень значимости (критичности) информации (УЗ) определяется степенью возможного ущерба от нарушения ее целостности (неправомерные уничтожение или модифицирование), доступности (неправомерное блокирование) или конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), в результате которого возможно нарушение штатного режима функционирования автоматизированной системы управления или незаконное вмешательство в процессы функционирования автоматизированной системы управления.

УЗ = [(целостность, степень ущерба) (доступность, степень ущерба) (конфиденциальность, степень ущерба)],

где степень возможного ущерба определяется заказчиком или оператором экспертным или иным методом и может быть:

высокой, если в результате нарушения одного из свойств безопасности информации (целостности, доступности, конфиденциальности), повлекшего нарушение штатного режима функционирования автоматизированной системы управления, возможно возникновение чрезвычайной ситуации федерального или межрегионального характера <*> или иные существенные негативные последствия в социальной, политической, экономической, военной или иных областях деятельности;

---

<*> Устанавливается в соответствии с постановлением Правительства Российской Федерации от 21 мая 2007 г. № 304 "О классификации чрезвычайных ситуаций природного и техногенного характера" (Собрание законодательства Российской Федерации, 2007, № 22, ст. 2640; 2011, № 21, ст. 2971).

средней, если в результате нарушения одного из свойств безопасности информации (целостности, доступности, конфиденциальности), повлекшего нарушение штатного режима функционирования автоматизированной системы управления, возможно возникновение чрезвычайной ситуации регионального или межмуниципального характера <*> или иные умеренные негативные последствия в социальной, политической, экономической, военной или иных областях деятельности;

---

<*> Устанавливается в соответствии с постановлением Правительства Российской Федерации от 21 мая 2007 г. № 304 "О классификации чрезвычайных ситуаций природного и техногенного характера" (Собрание законодательства Российской Федерации, 2007, № 22, ст. 2640; 2011, № 21, ст. 2971).

низкой, если в результате нарушения одного из свойств безопасности информации (целостности, доступности, конфиденциальности), повлекшего нарушение штатного режима функционирования автоматизированной системы управления, возможно возникновение чрезвычайной ситуации муниципального (локального) <*> характера или возможны иные незначительные негативные последствия в социальной, политической, экономической, военной или иных областях деятельности.

---

<*> Устанавливается в соответствии с постановлением Правительства Российской Федерации от 21 мая 2007 г. № 304 "О классификации чрезвычайных ситуаций природного и техногенного характера" (Собрание законодательства Российской Федерации, 2007, № 22, ст. 2640; 2011, № 21, ст. 2971).

В случае, если для информации, обрабатываемой в автоматизированной системе управления, не требуется обеспечение одного из свойств безопасности информации (в частности конфиденциальности) уровень значимости (критичности) определятся для двух других свойств безопасности информации (целостности, доступности). В этом случае:

УЗ = [(целостность, степень ущерба) (доступность, степень ущерба) (конфиденциальность, не применяется)].

Информация, обрабатываемая в автоматизированной системе управления, имеет высокий уровень значимости (критичности) (УЗ 1), если хотя бы для одного из свойств безопасности информации (целостности, доступности, конфиденциальности) определена высокая степень ущерба. Информация, обрабатываемая в автоматизированной системе управления, имеет средний уровень значимости (критичности) (УЗ 2), если хотя бы для одного из свойств безопасности информации (целостности, доступности, конфиденциальности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба. Информация, обрабатываемая в автоматизированной системе управления, имеет низкий уровень значимости (критичности) (УЗ 3), если для всех свойств безопасности информации (целостности, доступности, конфиденциальности) определены низкие степени ущерба.

При обработке в автоматизированной системе управления двух и более видов информации (измерительная информация, информация о состоянии процесса) уровень значимости (критичности) информации (УЗ) определяется отдельно для каждого вида информации. Итоговый уровень значимости (критичности) устанавливается по наивысшим значениям степени возможного ущерба, определенным для целостности, доступности, конфиденциальности каждого вида информации.

3. Класс защищенности автоматизированной системы управления определяется в соответствии с таблицей:

| Уровень значимости (критичности) информации | Класс защищенности автоматизированной системы управления |
|---|---|
| УЗ 1 | К1 |
| УЗ 2 | К2 |
| УЗ 3 | К3 |