**Лекция 10**

**Классификация объектов информатизации (ОИ) по требованиям ИБ**

Основные принципы классификации объектов информатизации:

1) однозначность - объект информатизации относится к одной категории;

2) обоснованность - достоверность оценки параметра характеристики категории при проведении классификации объекта информатизации, подтверждается документально либо путем фактического осмотра;

3) осведомленность - собственники или владельцы объектов информатизации информируются о классе объектов информатизации;

4) динамичность - класс объекта информатизации изменяется на протяжении срока его эксплуатации;

5) прозрачность - процедуры классификации объекта информатизации, категории, характеристики категории, параметры характеристики категории и индикаторы параметров характеристики категории четко описаны, однозначно и корректно трактуемы всеми субъектами информатизации.

ОИ можно классифицировать по определённым классам и рассматривать как типовые ОИ. К общим показателям относятся:

– важность информации;

– категория обрабатываемой информации;

– уровень защиты;

– контролируемая зона (КЗ);

– комплекс средств безопасности объекта (КСБО);

– условия функционирования при обработке информации (автономно или неавтономно).

Классификация ОИ, аттестуемых по требованиям ИБ, основана на иерархическом методе с использованием понятий "класс" и "подкласс".

В зависимости от важности обрабатываемой информации на ОИ устанавливаются:

подкласс 1 – сведения, отнесённые к государственным секретам (государственной тайне);

подкласс 2 – сведения ограниченного распространения;

подкласс 3 – открытая информация.

В зависимости от организации на ОИ вычислительного процесса устанавливаются:

подкласс А – технические средства (ТС) размещены в пределах одной контролируемой зоны (КЗ) и обработка защищаемой информации осуществляется в пределах области действия одного КСБО;

подкласс В – ТС размещены в нескольких КЗ и обработка защищаемой информации осуществляется в пределах области действия одного КСБО;

подкласс С – ТС размещены в пределах одной КЗ, обработка защищаемой информации осуществляется в пределах области действия одного КСБО, но ОИ имеет каналы обмена открытой информацией, выходящие за пределы КЗ.

При объединении подклассов ОИ образуется девять классов типовых объектов А1, А2, А3, В1, В2, В3, С1, С2, С3. Таким образом, по совокупности характеристик типового ОИ (идентичности объектов по назначению и условиям функционирования, подобия организации вычислительного процесса и области действий КСБО, идентичности по степени важности обрабатываемой на ОИ информации, видов угроз и задач безопасности) выделено девять иерархических классов по каждому из уровней защиты.

Для каждого класса предъявляются требования по обеспечению трех уровней защиты ОИ:

– базовая защита (предъявляются в том случае, если на ОИ обрабатывается открытая информация и требуется обеспечить высокую целостность и базовую доступность);

– расширенная защита (для данных с грифом секретно);

– повышенная защита (с грифом особой важности, совершенно секретно).

Учитывая, что для каждого класса предъявляются требования по обеспечению трех уровней защиты ОИ, мы получаем двадцать семь типовых ОИ, для которых необходимо разработать профили защиты.

Классификация производится по результатам идентификации.

Идентификация ОИ – определение принадлежности ОИ к одной из категорий классификатора;

Идентификация осуществляется путем отнесения объекта информатизации к наиболее подходящей по описанию категории.

Классификация основана на последовательном рассмотрении и оценке характеристик категории и параметров характеристик категории, относящихся к определенной категории.

Параметры характеристики категории в зависимости от уровня значимости делятся на:

1) ключевой - весовой коэффициент 1,5 балла;

2) основной - весовой коэффициент 1 балл;

3) базовый - весовой коэффициент 0,5 балла.

Суммарная оценка присваиваемых баллов индикаторов параметра характеристики категории, с учетом их весовых коэффициентов, определяет класс объекта информатизации.

**Классы защищенности государственной информационной системы**

Определение класса защищенности государственной информационной системы осуществляется в соответствии с **приказом ФСТЭК РФ № 17** "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" (от 11 февраля 2013 г.).

**Классы защищенности** ИС:

первый класс (К1),

второй класс (К2),

третий класс (К3)

Классы определяются в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой ИС, и ее масштаба – федеральный, региональный, объектовый.

УЗ информации определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от:

– нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение);

– целостности (неправомерные уничтожение или модифицирование);

– доступности (неправомерное блокирование) информации:

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

где степень возможного ущерба определяется обладателем информации (заказчиком) и (или) оператором самостоятельно экспертным или иными методами и может быть:

**– высокой**, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции;

– **средней**, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций;

**– низкой**, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

**Информация имеет высокий уровень** значимости (УЗ 1), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба.

**Информация имеет средний уровень значимости** (УЗ 2), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба.

**Информация имеет низкий уровень значимости** (УЗ 3), если для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба.

При обработке в информационной системе двух и более видов информации (служебная тайна, налоговая тайна и иные установленные законодательством Российской Федерации виды информации ограниченного доступа) уровень значимости информации (УЗ) определятся отдельно для каждого вида информации. Итоговый уровень значимости информации, обрабатываемой в информационной системе, **устанавливается по наивысшим значениям степени возможного ущерба**, определенным для конфиденциальности, целостности, доступности информации каждого вида информации.

Класс защищенности информационной системы определяется в соответствии с таблицей:



Зная УЗ и масштаб ИС, на пересечении строки и столбца определяем класс