ГОСУДАРСТВЕННЫЙ СТАНДАРТ
РЕСПУБЛИКИ БЕЛАРУСЬ

СТБ 34.101.30-2007

Информационные технологии
Методы и средства безопасности
ОБЪЕКТЫ ИНФОРМАТИЗАЦИИ
Классификация

Інфармацыйныя тэхналогіі
Метады і сродкі бяспекі
АБ'ЕКТЫ ІНФАРМАТЫЗАЦЫІ
Класіфікацыя

Издание официальное

63 9-2007

Госстандарт
Минск

УДК 004.056(083.74)(476) МКС 35.040 КП 05

Ключевые слова: технология информационная, безопасность, объект информатизации, объект типовой, классификация

Предисловие

Цели, основные принципы, положения по государственному регулированию и управлению в области технического нормирования и стандартизации установлены Законом Республики Беларусь «О техническом нормировании и стандартизации».

1 РАЗРАБОТАН государственным научным учреждением «Объединенный институт проблем информатики Национальной академии наук Беларуси» (ОИПИ НАН Беларуси)

ВНЕСЕН Государственным центром безопасности информации при Президенте Республики Беларусь (ГЦБИ)

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Госстандарта Республики Беларусь от 28 сентября 2007 г. № 49

3 ВВЕДЕН ВПЕРВЫЕ

Издан на русском языке

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ БЕЛАРУСЬ

Информационные технологии
Методы и средства безопасности
ОБЪЕКТЫ ИНФОРМАТИЗАЦИИ
Классификация

Інфармацыйныя тэхналогіі
Метады і сродкі бяспекі
АБ'ЕКТЫ ІНФАРМАТЫЗАЦЫІ
Класіфікацыя

Information technology
Security techniques
Objects of informatization
Classification

Дата введения 2009-04-01

1 Область применения

Настоящий стандарт устанавливает классификацию объектов информатизации по требованиям защиты обрабатываемой информации от несанкционированного доступа. Классификация объектов информатизации проводится с целью определения классов типовых объектов, для которых должны быть разработаны профили защиты.

Настоящий стандарт обеспечивает:

– развитие основных концептуальных положений СТБ 34.101.1 – СТБ 34.101.3 в области безопасности информационных технологий;

– единый методологический подход к классификации объектов информатизации по требованиям информационной безопасности;

– определение минимального числа профилей защиты объектов информатизации, которые должны быть разработаны в Республике Беларусь.

Настоящий стандарт применяется расположенными на территории Республики Беларусь:

– организациями, учреждениями и предприятиями независимо от форм собственности при проведении работ по защите активов на этапах проектирования, создания и эксплуатации объектов информатизации;

– заказывающими органами (потребителями) при подготовке профилей защиты для типовых объектов информатизации и заданий по обеспечению безопасности для конкретных реализаций объектов;

– другими физическими субъектами, занимающимися в инициативном порядке разработкой и обоснованием профилей защиты объектов информатизации различного назначения.

Требования настоящего стандарта не распространяются на продукты и системы информационных технологий, а охватывают объекты информатизации, на которых производится или планируется обработка информации и требуется защита их активов.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

СТБ 34.101.1-2004 (ИСО/МЭК 15408-1:1999) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

СТБ 34.101.2-2004 (ИСО/МЭК 15408-2:1999) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

СТБ 34.101.3-2004 (ИСО/МЭК 15408-3:1999) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности

Издание официальное

СТБ П ИСО/МЭК 17799-2000/2004 Информационные технологии и безопасность. Правила управления информационной безопасностью

Примечание – При пользовании настоящим стандартом целесообразно проверить действие технических нормативных правовых актов в области технического нормирования и стандартизации (далее – ТНПА) по каталогу, составленному по состоянию на 1 января текущего года, и по соответствующим информационным указателям, опубликованным в текущем году.
Если ссылочные ТНПА заменены (изменены), то при пользовании настоящим стандартом следует руководствоваться замененными (измененными) ТНПА. Если ссылочные ТНПА отменены без замены, то положение, в котором дана ссылка на них, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применяют термины, установленные в СТБ 34.101.1, а также следующие термины с соответствующими определениями:

3.1 активы: Информация или ресурсы, которые должны быть защищены средствами объекта информатизации.

3.2 доступность информации: Свойство информации быть доступной за приемлемое время по запросу со стороны санкционированного субъекта.

3.3 защита информации от несанкционированного доступа: Деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных нормативными правовыми актами, собственником или владельцем информации прав или правил доступа к защищаемой информации.

Примечание – Заинтересованным субъектом, осуществляющим несанкционированный доступ к защищаемой информации, могут выступать государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

3.4 контролируемая зона: Пространство (территория вокруг объекта информатизации, здание, часть здания), в пределах которого исключено неконтролируемое пребывание посторонних лиц и транспортных средств, не имеющих разрешения на постоянный или разовый доступ на объект.

3.5 конфиденциальность информации: Свойство информации, определяющее необходимую степень ее защиты от несанкционированного доступа и от использования ее субъектами, не имеющими соответствующих полномочий.

3.6 комплекс средств безопасности объекта информатизации: Совокупность аппаратных, программных и аппаратно-программных средств, на которые возлагается осуществление политики безопасности объекта информатизации.

Примечания
1 Под политикой безопасности объекта информатизации понимается совокупность правил, регулирующих управление активами, их защиту и распределение в объекте информатизации.
Политика информационной безопасности объекта информатизации является составной частью политики информационной безопасности организации.
2 Политика безопасности организации – совокупность правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности.

3.7 локальная вычислительная сеть: Совокупность средств вычислительной техники (персональных компьютеров и др.), находящихся на географически ограниченной территории, соединенных линиями связи, образованными кабелями, сетевыми адаптерами и другим коммуникационным оборудованием.

Примечание – Под географически ограниченной территорией понимают отдельное помещение в здании, здание либо здания, принадлежащие организации.

3.8 обработка информации: Совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования и отображения информации.

3.9 объект информатизации: Средства электронной вычислительной техники (автоматизированные системы различного уровня и назначения, вычислительные сети и центры, автономные стационарные и персональные электронные вычислительные машины, а также копировально-множительные средства, в которых для обработки информации применяются цифровые методы) вместе с программным обеспечением, которые используются для обработки информации.

3.10 средство безопасности: Аппаратное, программное, аппаратно-программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

3.11 средство защиты информации от несанкционированного доступа: Средство безопасности, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

3.12 степень важности информации: Обобщенный показатель, характеризующий степень обеспечения конфиденциальности, целостности и доступности обрабатываемой на объекте информации.

3.13 целостность информации: Свойство информации сохранять свое информационное содержание и однозначность интерпретации в условиях случайных и/или преднамеренных воздействий.

4 Обозначения и сокращения

В настоящем стандарте применяют следующие обозначения и сокращения:

КСБО – комплекс средств безопасности объекта;

ЛВС – локальная вычислительная сеть;

НСД – несанкционированный доступ;

ОИ – объект информатизации;

ПЭВМ – персональная электронно-вычислительная машина.

5 Общие положения

5.1 Объектом стандартизации является объект информатизации.

5.2 Защита ОИ от НСД является составной частью общей задачи обеспечения безопасности информации и осуществляется согласно правилам управления информационной безопасностью, приведенным в СТБ П ИСО/МЭК 17799, и требованиям режима секретности, действующим на ОИ. Определяющим свойством ОИ является степень конфиденциальности обрабатываемой информации.

5.3 Классификация проводится применительно к типовым ОИ. К типовым ОИ относятся объекты, оснащенные типовым набором аппаратных, программных, аппаратно-программных средств, в том числе и средств защиты информации.

5.4 Конкретная реализация объекта может отличаться от типового ОИ индивидуальными особенностями: конкретной реализацией функциональных требований безопасности, спецификацией и мерами гарантии безопасности.

5.5 Для каждого класса типового ОИ устанавливается базовый уровень защиты информации от НСД.

5.6 Базовый уровень защиты информации для типового ОИ характеризуется определенной минимальной совокупностью функциональных и гарантийных требований безопасности, обеспечивающих конфиденциальность, целостность и доступность обрабатываемой информации.

5.7 Требования по защите информации от НСД для типового ОИ представляются в профиле защиты типового объекта и описываются в виде набора функциональных и гарантийных требований безопасности в соответствии с СТБ 34.101.2 и СТБ 34.101.3.

5.8 Требования по защите информации от НСД для конкретной реализации ОИ определяются разработчиком ОИ и представляются в задании по безопасности в виде набора функциональных и гарантийных требований безопасности, спецификации средств защиты и мер гарантии в соответствии с СТБ 34.101.2 и СТБ 34.101.3.

В дополнение к требованиям безопасности информации (по отношению к базовому уровню) в задание по безопасности для конкретной реализации ОИ могут включаться требования более высокого уровня по СТБ 34.101.2 и СТБ 34.101.3, а также дополнительные требования, не входящие в указанные стандарты.

6 Классификация объектов информатизации по требованиям безопасности

6.1 В основу классификации ОИ положены следующие принципы:

– идентичности ОИ по степени конфиденциальности обрабатываемой на них информации;

– эквивалентности (подобия) ОИ по организации вычислительного процесса.

6.2 Устанавливаются следующие подклассы ОИ в зависимости от степени конфиденциальности обрабатываемой информации:

– подкласс 1 – совокупность объектов информатизации, на которых обрабатывается информация, содержащая сведения, отнесенные в установленном порядке к государственным секретам;

– подкласс 2 – совокупность объектов информатизации, на которых обрабатывается информация, содержащая сведения, отнесенные в установленном порядке к служебной информации ограниченного распространения, а также иная информация, охраняемая в соответствии с законодательством Республики Беларусь, за исключением сведений, отнесенных в установленном порядке к государственным секретам;

– подкласс 3 – совокупность объектов информатизации, на которых обрабатывается открытая информация.

6.3 Устанавливаются следующие подклассы ОИ в зависимости от организации на них вычислительного процесса:

– подкласс А – совокупность объектов информатизации, технические средства которых размещены в пределах одной контролируемой зоны и обработка защищаемой информации осуществляется в пределах области действия КСБО.

Примеры – Автономная ПЭВМ или ряд автономных ПЭВМ, размещенных в одном помещении; ЛВС; информационная система в виде взаимодействующих между собой ЛВС, автоматизированных рабочих мест и др.;

– подкласс Б – совокупность объектов информатизации, технические средства которых размещены в нескольких контролируемых зонах, объединенных открытыми или защищенными каналами передачи данных, и обработка информации осуществляется в пределах области действия КСБО.

Пример – ОИ, представляющие собой корпоративную вычислительную сеть, т.е. более двух вычислительных сетей или отдельных ПЭВМ, объединенных между собой защищенными каналами передачи данных.

– подкласс В – совокупность объектов информатизации, технические средства которых размещены в одной контролируемой зоне и обработка защищаемой информации осуществляется в пределах области действия КСБО, но один или несколько из совокупности объектов имеет (имеют) каналы обмена информацией, выходящие за пределы контролируемой зоны.

Пример – ОИ, представляющие собой ЛВС или ПЭВМ, подключенные к сетям общего пользования (например, Интернет), и обрабатывающие защищаемую информацию без ее передачи другим, внешним ОИ.

6.4 Устанавливаются следующие классы типовых объектов информатизации, для которых необходимо разработать профили защиты:

– класс А1 – совокупность объектов информатизации, на которых обрабатывается информация в пределах области действия КСБО, содержащая сведения, отнесенные в установленном порядке к государственным секретам, технические средства которых размещены в пределах одной контролируемой зоны;

– класс Б1 – совокупность объектов информатизации, на которых обрабатывается информация в пределах области действия КСБО, содержащая сведения, отнесенные в установленном порядке к государственным секретам, технические средства которых размещены в нескольких контролируемых зонах, объединенных защищенными каналами передачи данных;

– класс В1 – для данного класса профиль защиты не разрабатывается, так как объекты информатизации, обрабатывающие информацию, содержащую сведения, отнесенные в установленном порядке к государственным секретам, не должны иметь каналов обмена информацией за пределами контролируемой зоны;

– класс А2 – совокупность объектов информатизации, на которых обрабатывается информация в пределах области действия КСБО, содержащая сведения, отнесенные в установленном порядке к служебной информации ограниченного распространения, технические средства которых размещены в пределах одной контролируемой зоны;

– класс Б2 – совокупность объектов информатизации, на которых обрабатывается информация в пределах области действия КСБО, содержащая сведения, отнесенные в установленном порядке к служебной информации ограниченного распространения, технические средства которых размещены в нескольких контролируемых зонах, объединенных защищенными каналами передачи данных;

– класс В2 – для данного класса профиль защиты не разрабатывается, так как объекты информатизации, обрабатывающие служебную информацию ограниченного распространения, не должны иметь каналов обмена информацией за пределами контролируемой зоны;

– класс А3 – совокупность объектов информатизации, на которых обрабатывается открытая информация в пределах области действия КСБО, технические средства которых размещены в пределах одной контролируемой зоны;

– класс Б3 – совокупность объектов информатизации, на которых обрабатывается открытая информация в пределах области действия КСБО, технические средства которых размещены в нескольких контролируемых зонах, объединенных открытыми или защищенными каналами передачи данных;

– класс В3 – совокупность объектов информатизации, на которых обрабатывается открытая информация в пределах области действия КСБО, технические средства которых размещены в пределах одной контролируемой зоны, но имеющие каналы обмена информацией за пределами контролируемой зоны.

Ответственный за выпуск *В.Л. Гуревич*

Сдано в набор 09.10.2007. Подписано в печать 12.11.2007. Формат бумаги 60×84/8. Бумага офсетная.
Гарнитура Arial. Печать ризографическая. Усл. печ. л. 0,58 Уч.-изд. л. 0,41 Тираж экз. Заказ

Издатель и полиграфическое исполнение
НП РУП «Белорусский государственный институт стандартизации и сертификации» (БелГИСС)
Лицензия № 02330/0133084 от 30.04.2004.
220113, г. Минск, ул. Мележа, 3.