УДК 621.391

ОПЫТ СОЗДАНИЯ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

А.А. ОБУХОВИЧ, М.Н. БОБОВ

ОАО «АГАТ-системы управления» – управляющая компания холдинга «Геоинформационные системы управления»
пр-т Независимости, 117, г. Минск, 220114, Республика Беларусь

Работы по обеспечению защиты информации в информационных автоматизированных системах проводятся на предприятии с 1974 года.

За 40 лет проведено 24 научно-исследовательские работы, результаты которых легли в основу методологии защиты информации в информационных автоматизированных системах.

На основе разработанной методологии создано более 100 систем военного и гражданского назначения. В частности разработаны, внедрены и аттестованы системы защиты информации в государственных межведомственных информационных системах ОАИС, ЕИС КВП, ИАС КНД и ведомственных информационных системах ИСУ Госкомвоенпрома, ИАС УВК и др.

Разработанная методология устанавливает порядок и содержание работ по обеспечению защиты информации на протяжении всего жизненного цикла информационных систем и определяет соответствующее каждому этапу нормативно-методическое обеспечение. Опыт показывает, что методология позволяет обеспечить гарантированность защиты информации, унификацию требований, предъявляемых к средствам и системам защиты, их совместимость при использовании в системах различного уровня и назначения, повышение качества разработки средств защиты и защищаемых систем при одновременном снижении трудоемкости работ, исключении дублирования работ и сокращения общей номенклатуры нормативно-методической документации.

Разработанный в соответствии с методологией пакет нормативно- методических документов состоит из трёх основных групп, включающих в себя документы организационно-системного плана, документы, определяющие порядок разработки, внедрения и приемки защищенных систем, и документы оценке уровня защищенности информации в системах.

Структура и состав разработанных нормативно-методических документов базируются на основных принципах, сформулированных ниже.

Первым принципом является разработка положений нормативно-методических документов исходя из расчета на «худший случай», т.е. документы предполагают задание самых жестких требований и указания условий, когда эти требования могут быть смягчены или носят рекомендательный характер.

Вторым принципом является организационная совместимость документов с действующими государственными стандартами в данной и смежных областях.

Третьим принципом является соблюдение единой терминологии, принятой в данной предметной области.

Четвертым принципом является первоочередность разработки организационно-методических документов, регламентирующих порядок проведения работ по защите информации и взаимоотношения участников создания защищенных систем.

Документы организационно-системного плана являются наиболее важной группой документов, т.к. именно они определяют основные положения по защите информа-

ции при ее электронной обработке, терминологию, используемую в этой области техники, и систему технической документации по защите информации.

Ко второй группе относятся документы, определяющие порядок разработки, испытаний, внедрения и приемки защищённых систем. Эти документы определяют состав и содержание работ по стадиям создания защищенных систем, так как в процессе их создания, внедрения и эксплуатации принимает участие значительное количество заинтересованных сторон: заказчики, головные разработчики, соисполнители, представители специализированных организаций, изготовители и потребители. Регламентация их прав и обязанностей на всех стадиях жизненного цикла систем также является задачей документов данной группы. К этой же группе относятся и типовые проектные решения по защите информации.

К третьей группе относятся документы, регламентирующие работы по оценке уровня защищенности информации в системах.

На основе документов организационно-системного плана при создании защищенных систем производятся следующие важнейшие работы:

– определение объектов защиты в системе;

– формирование правил разграничения доступа к ресурсам системы;

– разработка модели нарушителя;

– обоснованию критериев защищенности информационной системы;

– обоснованию требований безопасности к системе.

Документы второй группы в основном используются:

– при разработке технического задания на систему защиты информации;

– при разработке комплекса мер по реализации гарантийных требований безопасности по СТБ 34.101.3;

– при выборе средств, реализующих функциональные требования безопасности.

Документы по оценке защищенности определяют показатели и критерии защищенности, методики категорирования защищаемых ресурсов системы, методики оценки средств и систем защиты. Документы этой группы используют:

– для оценки и обработки информационных рисков;

– для оценки соответствия разработанных средств требованиям технических нормативных правовых актов по защите информации;

– для инженерной оценки стойкости к преодолению или обходу средств защиты;

– для аттестации информационной системы по требованиям информационной безопасности.

Опыт работы в области защиты информации показал, что эффективное создание защищенных информационных систем возможно только при использовании принятой методологии защиты, действующей в виде комплекса стандартов предприятия-разработчика.