Обеспечение безопасности информации на различных уровнях применения защищенных информационных технологий

И. С. Свирин,
начальник отдела ОАО «ВНИИНС», кандидат технических наук,

А. А. Тагиев,
заместитель начальника службы безопасности ОАО «ВНИИНС»

Внедрение защищенных информационных технологий в процессы обработки информации является сложным многоэтапным процессом.

На начальном этапе основные усилия разработчиков были направлены на создание средств вычислительной техники (СВТ), ориентированных на удовлетворение потребностей отдельных должностных лиц (автоматизация простейших процессов, подготовка документов в однопользовательском режиме и др.).

Следующий этап направлен на автоматизацию деятельности органов управления, когда задачи, решаемые отдельными должностными лицами, являются составной частью сложных процессов коллективной обработки информации. Для этого было необходимо объединение отдельных средств вычислительной техники в автоматизированные системы (АС), что в свою очередь потребовало разработку дополнительных средств защиты информации.

Создание объектов автоматизации диктует необходимость проработки дополнительных вопросов, связанных с обеспечением защиты от утечек информации по техническим каналам, в т.ч. с использованием специализированных информационных технологий, основанных на использовании криптографических методов.

Эффективное решение задач управления возможно только при обеспечении защищенного высокоскоростного взаимодействия между различными структурами в рамках единой информационной системы. Это требует проработки вопросов межобъектового взаимодействия, как с точки зрения защиты информации, так и с точки зрения сопряжения гетерогенных вычислительных и информационных сред (протоколы, форматы структур данных и др.).

Уровни применения информационных технологий

Средства вычислительной техники

Основой отечественной нормативной базы для создания средств вычислительной техники являются руководящие документы ФСТЭК России, которые устанавливают термины и определения понятий в области защиты СВТ и АС от несанкционированного доступа, описывают требования по безопасности, вводят классификацию СВТ по уровню защищенности от несанкционированного доступа (НСД) к информации на базе перечня показателей защищенности и совокупности описывающих их требований и пр.

Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» излагает систему взглядов и основные принципы, которые закладываются в основу проблемы защиты информации от несанкционированного доступа, являющейся частью общей проблемы безопасности информации. Документ является методологической базой нормативно-технических и методических документов, направленных на решение следующих задач:

- выработки требований по защите СВТ и АС от НСД к информации;
- создания защищенных от НСД к информации СВТ и АС;
- сертификации защищенных СВТ и АС.

Данный документ предусматривает существование двух самостоятельных направлений в проблеме защиты информации от НСД: направление, связанное с СВТ, и направление, связанное с АС. Отличие порождено тем, что СВТ разрабатываются и поставляются лишь как элементы, из которых в дальнейшем строятся функционально ориентированные АС, и поэтому, не решая прикладных задач, СВТ не содержат пользовательской информации. Помимо пользовательской информации при создании АС появляются такие характеристики, как полномочия пользователей, модель нарушителя, технология обработки информации. В связи с этим если понятия защищенность информации от НСД в АС и защищенность АС от НСД к информации эквивалентны, то в случае СВТ можно говорить лишь о защищенности СВТ от НСД к информации, для обработки, хранения и передачи которой оно предназначено. При этом защищенность СВТ есть потенциальная защищенность, т.е. свойство предотвращать или существенно затруднять НСД к информации в дальнейшем при использовании СВТ в АС.

Защита информации на уровне СВТ реализована во всех изделиях базовых информационных защищенных компьютерных технологий (БИЗКТ), разработанных ОАО «ВНИИНС». Основным принципом реализации средств защиты информации (СЗИ) СВТ является принцип минимизации дублирования функциональности, поэтому СЗИ СВТ более высокого уровня обязательно базируются на СЗИ СВТ нижних уровней, например, СЗИ СУБД «Линтер ВС» 6.0 опирается на СЗИ ОС МСВС 3.0, а специальное программное обеспечение, взаимодействующее с СУБД, максимально использует СЗИ СУБД. При этом каждое СВТ может иметь некоторые собственные средства защиты, определяемые его спецификой. Например, СУБД «Линтер ВС» 6.0 имеет встроенные средства разграничения доступа, что связано с отсутствием в ОС МСВС 3.0 таких объектов доступа, как таблицы, строки таблиц или поля записей.

Автоматизированные системы

Основным документом, регламентирующим правила построения АС ВН, является Руководящий документ ФСТЭК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требований по защите информации», устанавливающий классификацию АС, подлежащих защите от НСД к информации, и требования по защите информации в АС различных классов. Классификация распространяется на все действующие и проектируемые АС, обрабатывающие информацию, содержащую государственную тайну. Выбор класса АС производят заказчик и разработчик с привлечением специалистов по защите информации.

Руководящий документ «Положение по организации разработки, из-

готовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники» устанавливает единый на территории Российской Федерации порядок исследований и разработок в области:

- защиты информации, обрабатываемой АС различного уровня и назначения, от несанкционированного доступа;
- создания СВТ, защищенных от утечки, искажения или уничтожения информации за счет НСД, в том числе программных и технических средств защиты информации от НСД;
- создания программных и технических средств защиты информации от НСД в составе систем защиты секретной информации в создаваемых АС.

Положение обязательно для выполнения всеми органами государственного управления, государственными предприятиями, учреждениями, организациями и предприятиями, обладающими государственными секретами, и предназначено для заказчиков, разработчиков и пользователей защищенных СВТ, автоматизированных систем, функционирующих с использованием информации различной степени секретности.

Требования указанных нормативных документов учтены ОАО «ВНИИНС» в ходе создания базовых информационных защищенных компьютерных технологий (БИЗКТ), а существующие информационные технологии уже сегодня позволяют создавать защищенные СВТ и защищенные автоматизированные системы.

Однако **существующая нормативная база существенно устарела и не отвечает современным требованиям к защищенным АС. Разработки ОАО «ВНИИНС» в области средств защиты информации учитывают актуальные тенденции** и направлены:

- на обеспечение программной, технической совместимости АС и совместимости АС по СЗИ;
- на применение распределенной системы хранения и обработки данных, а также типовых программно-технических комплексов для обеспечения возможности интеграции АС в единую иерархическую сеть управления;
- на обеспечение возможности интеграции автоматизированных систем (подсистем) управления различного назначения;
- на обеспечение информационного взаимодействия указанных АСУ;
- на обеспечение возможности построения систем управления и защиты информации, территориально разнесенных сложных АС с централизованным и децентрализованным управлением.

Информационные технологии объектового назначения

Организация и проведение мероприятий по специальной защите должны предусматриваться и выполняться на всех этапах функционирования объекта от разработки технического задания до этапа повседневной эксплуатации.

Для обработки информации должны использоваться сертифицированные серийно выпускаемые в защищенном исполнении технические средства (ТС), а также образцы ТС, прошедшие специальные исследования и имеющие предписания на эксплуатацию.

Для защиты информации от утечки по техническим каналам должны использоваться сертифицированные средства защиты информации. Обработка информации без принятия необходимых мер по ее защите от утечки по техническим каналам запрещается.

В целях разработки и принятия обоснованных мер спецзащиты все объекты должны быть отнесены к соответствующим категориям. Категории устанавливаются в зависимости от степени секретности обрабатываемой информации и условий расположения объектов.

При необходимости на объектах устанавливаются технические средства охраны, в состав которых включены технические средства, имеющие заключения и предписания на эксплуатацию.

Основные тенденции развития технологий объектового назначения связаны со следующими направлениями:

- создание линейки отечественных средств технической охраны, основанных на использовании технологий интеллектуальной обработки мультимедийной информации (потоков видеоданных, акустических сигналов, информации от извещателей и др.);
- объединение программных и программно-технических средств объектового назначения в единый контур управления, построеный по принципу «интеллектуального здания»;
- использование методов математического и имитационного моделирования для повышения эффективности проведения специальных исследований категорированных объектов и упрощения процедуры их модернизации.

Системные решения

Развитие телекоммуникационных средств и создание территориально-распределенных информационных сетей существенно изменили процессы сбора, хранения, представления и обработки информации. Современная стадия характеризуется переносом акцента на обеспечение взаимодействия между децентрализованно протекающими процессами обработки информации. Происходит переход от автономной обработки различных видов информации к интегрированной, обеспечивающей пользователю доступ к различным информационным ресурсам.

Работы последних десятилетий по повышению качества информационной поддержки процессов управления сосредотачивались главным образом на создании технических средств, автоматизированных и телекоммуникационных систем, предназначенных для обработки и передачи информации. При этом ставилась задача обеспечения возможности оперативного и целенаправленного использования информации на основе внедрения современных информационных технологий. Однако по-прежнему остается актуальным вопрос обеспечения полноты и своевременности предоставления информации, необходимой для решения задач управления. В то же время созданные автоматизированные системы управления, а также телекоммуникационные системы нередко недогружены и используются неэффективно.

Современное состояние науки и техники позволяет приступить к созданию элементов Единого информационного пространства (ЕИП), рассматриваемого как автоматизированный аналог усовершенствованного и упорядоченного информационного пространства. ЕИП должно стать одной из важнейших составляющих единого информационного пространства России, обладая при этом определенной самостоятельностью, ввиду специфики, содержащейся в нем информации. Таким образом, развитие системного уровня применения информационных технологий продиктовано следующими группами требований:

1. Общие требования по созданию ЕИП:

- использование единых средств формирования, ведения, хранения, интеграции и представления информационных ресурсов БИЗКТ;
- реализация общесистемного программного обеспечения в среде БИЗКТ;
- использование ОПО, СЗИ, а также СПО общего применения, функ-

ционирующего в среде БИЗКТ на базе унифицированного общесистемного программного обеспечения;
- использование средств управления ресурсами ЕИП и обеспечения повседневной деятельности должностных лиц, позволяющих создание интегрированных информационных ресурсов и АС;
- использование единых системотехнических решений для ведения и поддержания системы классификации и кодирования, нормативно-справочной информации, информационной базы и унифицированной системы форм документов.

2. Общие требования к построению системы обеспечения безопасности информации ЕИП:
- система защиты информации должна создаваться на единых принципах, обеспечивая сопряжение и оперативное управление (централизованное и децентрализованное) ею на различных уровнях;
- построение системы защиты должно базироваться на модульном принципе с возможностью ее наращивания в зависимости от звена управления, степени секретности обрабатываемой информации, режима обработки (коллективной или индивидуальной) и решаемых задач.

Комплексные системы обеспечения безопасности информации, разработанные ОАО «ВНИИНС»

Комплекс средств защиты информации от несанкционированного доступа

Комплекс средств защиты информации от несанкционированного доступа (КСЗИ НСД) предназначен для обеспечения возможности построения системы защиты информации от несанкционированного доступа автоматизированной системы, обрабатывающей информацию с максимальной степенью секретности — «совершенно секретно», и соответствующей требованиям РД Гостехкомиссии России, отнесенным к классу защищенности АС — 1Б.

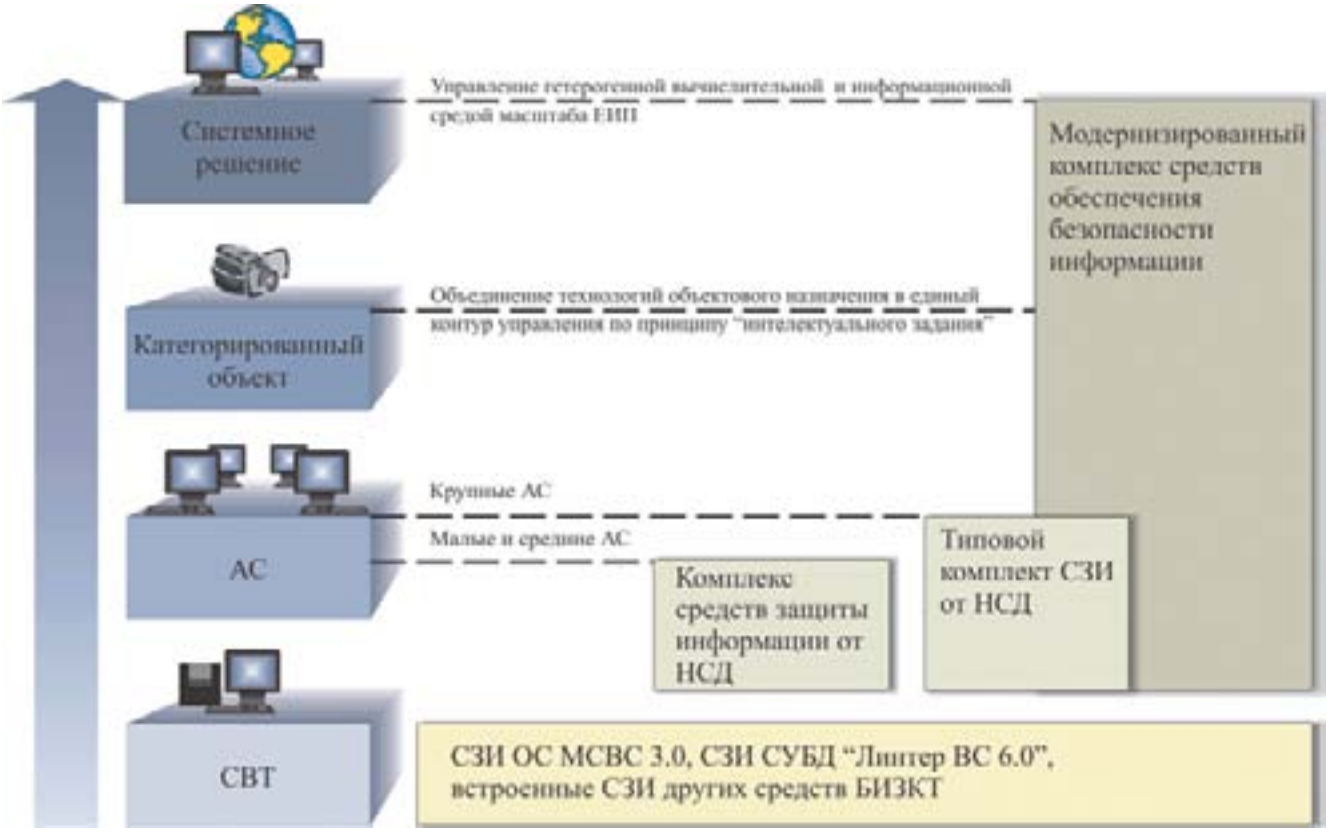
КСЗИ НСД обеспечивает выполнение следующих функций:
- централизованное управление СЗИ от НСД в рамках АС;
- обеспечение централизованного контроля доступа к защищаемым ресурсам АС;
- управление учетными записями пользователей;
- установка и модификация меток конфиденциальности объектов доступа;
- тиражирование производимых настроек на определенные администратором безопасности рабочие станции из состава АС;
- регистрация попыток НСД, т.е. действий, не разрешенных в соответствии с правилами разграничения доступа ОС МСВС 3.0;
- регистрация действий администратора безопасности по изменению правил разграничения доступа;
- периодический контроль целостности файлов по именам и контрольным суммам в процессе работы ОС.

КСЗИ НСД представляет собой комплексную систему обеспечения безопасности, ориентированную на малые и средние объекты автоматизации с низким уровнем интеграции управляемых компонентов СЗИ. Изделие обеспечивает управление СЗИ СВТ, входящих в состав АС, а также предоставляет программный интерфейс для расширения своих функциональных возможностей по управлению перспективными (разрабатываемыми) СЗИ.

Типовой комплект СЗИ от НСД

Особое значение безопасность информации приобретает в объектах с распределенной структурой, не имеющих хорошо спланированной и организованной физической защиты и использующих ненадежные, потенциально доступные злоумышленнику каналы связи.

На объектах такого типа практически вся ответственность за безопасность информации возлагается на программное обеспечение, поэто-



му при разработке и эксплуатации таких АС возникает потребность в информационных технологиях, обеспечивающих защиту информационных потоков в распределенной компьютерной сети. Такую технологию представляет изделие «Типовой комплект СЗИ от НСД». Данное изделие обеспечивает создание логически связанных управляемых доменных структур и имеет следующие особенности:

- единый периметр безопасности компьютерной сети за счет применения централизованных механизмов управления и контроля, наличия единого пространства пользователей;
- обеспечение доступности информации в сети за счет использования унифицированного механизма синхронизации информационных потоков внутри домена;
- контроль распределенной системы за счет использования унифицированной системы аудита домена;
- обеспечение управляемости и быстрого реагирования в распределенной компьютерной сети за счет применения унифицированной системы управления доменом;
- обеспечение целостности информации за счет интегрированных механизмов контроля целостности в домене;
- встроенные механизмы обеспечения безопасной печати конфиденциальных документов;
- встроенный механизм генерации и распределения паролей;
- встроенное прикладное программное обеспечение для решения типовых задач информационной безопасности: антивирусное ПО, ПО резервного копирования, ПО удаленного восстановления и др.

Типовой комплект СЗИ от НСД функционирует на аппаратных платформах Intel, Sparc и Mips.

Типовой комплект СЗИ от НСД представляет собой комплексную систему обеспечения безопасности, ориентированную на малые и средние объекты автоматизации.

Модернизированный комплекс средств обеспечения безопасности информации (МК СОБИ)

Модернизированный комплекс средств обеспечения безопасности информации (МК СОБИ) предназначен для управления и мониторинга сложных масштабных АС и ориентирован на сокращение затрат на эксплуатацию за счет уменьшения численности обслуживающего персонала.

При создании МК СОБИ учтена гетерогенность используемых в составе АС информационных технологий, которые потенциально могут быть разработаны различными производителями для разных программных и аппаратных платформ. МК СОБИ представляет собой комплексную систему управления информационными технологиями, осуществляющую интеграцию СЗИ в единый комплекс.

При построении МК СОБИ для управления СЗИ распределенной системы использована многоуровневая архитектура, в которой нижние уровни предоставляют услуги соседним высшим уровням. Можно выделить следующие уровни архитектуры управления СЗИ:

- прикладной уровень;
- уровень системы управления;
- уровень служб (сервисов) домена;
- уровень ядра домена;
- уровень промежуточного программного обеспечения.

Прикладной уровень представляет собой специальное программное обеспечение, реализующее целевую функцию АС.

Специальное программное обеспечение пользуется услугами систем, представленными уровнем системы управления. Каждая система управления может иметь свои функциональные особенности. Например, одна может быть предназначена для управления сетевой инфраструктурой, другая — для управления рабочими местами пользователей и т.д. Каждая из них представляет собой законченное программное средство, отвечающее определенным требованиям.

Функциональность системы управления обуславливается использованием тех или иных служб, которые предоставляет уровень служб (сервисов) домена. Каждая служба представляет собой обособленный функционально завершенный элемент, который выполняет определенные типовые задачи. Набор служб не является фиксированным и может расширяться с появлением новых задач, которые могут быть применены в системах.

Основным уровнем, представляющим собой основу системы, является уровень ядра домена. Он предоставляет базовые механизмы управления и контроля элементов СЗИ.

Данный уровень, в свою очередь, должен базироваться на промежуточном уровне, представляющем собой промежуточное программное обеспечение. Он является платформой для построения и функционирования защищенных распределенных программных средств. На данный уровень вынесены такие важные системные вопросы, как безопасность передачи данных, кроссплатформенность, удаленное взаимодействие компонентов системы, резервирование серверов на случай отказа, разграничение доступа к функциям системы. Данный уровень представляет платформонезависимый слой, реализуя взаимодействие с платформозависимым слоем, на котором функционирует общее программное обеспечение.

Основой интеграции СЗИ в распределенных АС является централизованный контроль и управление. Объединение в домены позволяет структурировать сложную распределенную систему, выделить локальные центры управления, а также построить вертикаль управления. В такой модели объединяемые и управляемые СЗИ являются объектами управления. Объектами управления могут быть и технические средства, такие как сетевое оборудование или элементы интегрированной системы физической безопасности объекта автоматизации.

Реализация на базе МК СОБИ системы управления СЗИ, организованной по доменному принципу с использованием расширяемых функциональных возможностей сервисов доменов, построенной на основе компонентной модели платформонезависимого распределенного программного обеспечения промежуточного слоя, позволила ОАО «ВНИИНС» выполнить взаимную интеграцию элементов СЗИ средств БИЗКТ, а также осуществлять централизованный контроль и управление всеми программными и аппаратными средствами в распределенной гетерогенной среде.

Использование разработанных в ОАО «ВНИИНС» комплексных систем обеспечения безопасности информации позволяет выполнить построение единого контура управления СЗИ на всех уровнях применения информационных технологий от отдельных СВТ до сложных системных решений.

ОАО «ВНИИНС»
Россия, 117638, г. Москва
Сивашская ул., д. 4, корп. 2
Тел.: (499) 619-6842
Факс: (495) 310-7097
E-mail: vniins@vniins.ru