Руководящий документ.
Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.

Утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

Принятые сокращения

АС - автоматизированная система
КСЗ - комплекс средств защиты
НСД - несанкционированный доступ
ОС - операционная система
ППП - пакет прикладных программ
ПРД - правила разграничения доступа
РД - руководящий документ
СВТ - средства вычислительной техники
СЗИ - система защиты информации
СЗИ НСД - система защиты информации от несанкционированного доступа
СЗСИ - система защиты секретной информации
СНТП - специальное научно-техническое подразделение
СРД - система разграничения доступа
СУБД - система управления базами данных
ТЗ - техническое задание
ЭВМ - электронно-вычислительная машина
ЭВТ - электронно-вычислительная техника

1.Общие положения

1.1. Настоящий документ излагает систему взглядов, основных принципов, которые закладываются в основу проблемы защиты информации от несанкционированного доступа (НСД), являющейся частью общей проблемы безопасности информации.

1.2. Концепция предназначена для заказчиков, разработчиков и пользователей СВТ и АС, которые используются для обработки, хранения и передачи требующей защиты информации.

1.3. Концепция является методологической базой нормативно-технических и методических документов, направленных на решение следующих задач:

выработка требований по защите СВТ и АС от НСД к информации;

создание защищенных от НСД к информации СВТ и АС;

сертификация защищенных СВТ и АС.

1.4. Концепция предусматривает существование двух относительно самостоятельных и, следовательно, имеющих отличие направлений в проблеме защиты информации от НСД: направление, связанное с СВТ, и направление, связанное с АС.

Отличие двух направлений порождено тем, что СВТ разрабатываются и поставляются на рынок 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 отсутствующие при разработке СВТ характеристики АС, как полномочия пользователей, модель нарушителя, технология обработки информации.

В связи с этим, если понятия защищенность (защита) информации от НСД в АС и защищенность (защита) АС от НСД к информации эквивалентны, то в случае СВТ можно говорить лишь о защищенности (защите) 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.

2. Определение НСД

2.1. При анализе общей проблемы безопасности информации выделяются те направления, в которых преднамеренная или непреднамеренная деятельность человека, а также неисправности технических средств, ошибки программного обеспечения или стихийные бедствия могут привести к утечке, модификации или уничтожению информации.

Известны такие направления исследования проблемы безопасности информации, как радиотехническое, побочные электромагнитные излучения и наводки, акустическое, НСД и др.

2.2. НСД определяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС.

Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС.

3. Основные принципы защиты от НСД

3.1. Защита СВТ и АС основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите от НСД к информации.

3.2. Защита СВТ обеспечивается комплексом программно-технических средств.

3.3. Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.

3.4. Защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

3.5. Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС).

3.6. Неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.

3.7. Защита АС должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами.

4. Модель нарушителя в АС

4.1. В качестве нарушителя рассматривается субъект, имеющий доступ к работе со штатными средствами АС и СВТ как части АС.

Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ. Выделяется четыре уровня этих возможностей.

Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

4.2. Первый уровень определяет самый низкий уровень возможностей ведения диалога в АС - запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяется возможностью управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.

Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

4.3. В своем уровне нарушитель является специалистом высшей квалификации, знает все об АС и, в частности, о системе и средствах ее защиты.

5. Основные способы НСД

К основным способам НСД относятся:

непосредственное обращение к объектам доступа;

создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;

модификация средств защиты, позволяющая осуществить НСД;

внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД.

6. Основные направления обеспечения защиты от НСД

6.1. Обеспечение защиты СВТ и АС осуществляется:

системой разграничения доступа (СРД) субъектов к объектам доступа;

обеспечивающими средствами для СРД.

6.2. Основными функциями СРД являются:

реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным;

реализация ПРД субъектов и их процессов к устройствам создания твердых копий;

изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;

управление потоками данных в целях предотвращения записи данных на носители несоответствующего грифа;

реализация правил обмена данными между субъектами для АС и СВТ, построенных по сетевым принципам.

6.3. Обеспечивающие средства для СРД выполняют следующие функции:

идентификацию и опознание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;

регистрацию действий субъекта и его процесса;

предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;

реакцию на попытки НСД, например, сигнализацию, блокировку, восстановление после НСД;

тестирование;

очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;

учет выходных печатных и графических форм и твердых копий в АС;

контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств.

6.4. Ресурсы, связанные как с СРД, так и с обеспечивающими ее средствами, включаются в объекты доступа.

6.5. Способы реализации СРД зависят от конкретных особенностей СВТ и АС. Возможно применение следующих способов защиты и любых их сочетаний:

распределенная СРД и СРД, локализованная в программно-техническом комплексе (ядро защиты);

СРД в рамках операционной системы, СУБД или прикладных программ;

СРД в средствах реализации сетевых взаимодействий или на уровне приложений;

использование криптографических преобразований или методов непосредственного контроля доступа;

программная и (или) техническая реализация СРД.

7. Основные характеристики технических средств защиты от НСД

7.1. Основными характеристиками технических средств защиты являются:

степень полноты и качество охвата ПРД реализованной СРД;

состав и качество обеспечивающих средств для СРД;

гарантии правильности функционирования СРД и обеспечивающих ее средств.

7.2. Полнота и качество охвата ПРД оценивается по наличию четких непротиворечивых заложенных в СРД правил доступа к объектам доступа и мерам их надежной идентификации. Учитываются также возможности контроля разнообразных дисциплин доступа к данным.

7.3. При оценке состава и качества обеспечивающих средств для СРД учитываются средства идентификации и опознания субъектов и порядок их использования, полнота учета действий субъектов и способы поддержания привязки субъекта к его процессу.

7.4. Гарантии правильности функционирования оцениваются по способам проектирования и реализации СРД и обеспечивающих ее средств (формальная и неформальная верификация) и по составу и качеству препятствующих обходу СРД средств (поддержание целостности СРД и обеспечивающих средств, восстановление после сбоев, отказов и попыток НСД, контроль дистрибуций, возможность тестирования на этапе эксплуатации).

7.5. Оцениваемые АС или СВТ должны быть тщательно документированы. В состав документации включаются Руководство пользователя по использованию защитных механизмов и Руководство по управлению средствами защиты. Для АС и СВТ, претендующих на высокий уровень защищенности, оценка осуществляется при наличии проектной документации (эскизный, технический и рабочий проекты), а также описаний процедур тестирования и их результатов.

8. Классификация АС

8.1. Классификация необходима для более детальной, дифференцированной разработки требований по защите от НСД с учетом специфических особенностей этих систем.

8.2. В основу системы классификации АС должны быть положены следующие характеристики объектов и субъектов защиты, а также способов их взаимодействия:

информационные, определяющие ценность информации, ее объем и степень (гриф) конфиденциальности, а также возможные

последствия неправильного функционирования АС из-за искажения (потери) информации;

организационные, определяющие полномочия пользователей;

технологические, определяющие условия обработки информации, например, способ обработки (автономный, мультипрограммный и т.д.), время циркуляции (транзит, хранение и т.д.), вид АС (автономная, сеть, стационарная, подвижная и т.д.).

9. Организация работ по защите от НСД

9.1. Организация работ по защите СВТ и АС от НСД к информации должна быть частью общей организации работ по безопасности информации.

9.2. Обеспечение защиты основывается на требованиях по защите к разрабатываемым СВТ и АС, формулируемых заказчиком и согласуемых с разработчиком.

Эти требования задаются либо в виде желаемого уровня защищенности СВТ или АС, либо в виде определенного, соответствующего этому уровню перечня требований.

Требования по защите обеспечиваются разработчиком в виде комплекса средств защиты. Организационные мероприятия для АС реализуются заказчиком.

Ответственность за разработку КСЗ возлагается на главного конструктора СВТ или АС.

9.3. Проверка выполнения технических требований по защите проводится аналогично с другими техническими требованиями в процессе испытаний (предварительных, государственных и др.).

По результатам успешных испытаний оформляется документ (сертификат), удостоверяющий соответствие СВТ или АС требованиям по защите и дающий право разработчику на использование и (или) распространение их как защищенных.

9.4. Разработка мероприятий по защите должна проводиться одновременно с разработкой СВТ и АС и выполняться за счет финансовых и материально-технических средств (ресурсов), выделенных на разработку СВТ и АС