Лекция №3

С.А. Краснов

Формирование требований к системе информационной безопасности

# Формирование требований к системе информационной безопасности

Лекция №3.

Тема №1: Основные понятия и задачи программно-аппаратной защиты информации, принципы её построения.

Тема лекции: Формирование требований к системе информационной безопасности.

**Изучаемые вопросы:**

1. Требования к системе информационной безопасности и классы защищенности АС от НСД к информации;

2. Классификация средств вычислительной техники по защищенности от НСД к информации.

## Требования к системе информационной безопасности и классы защищенности АС от НСД к информации

Перед разработкой системы информационной безопасности должны быть сформированы требования по защите информации. Кроме того, необходимо уточнение этих требований после формирования моделей защищаемых ресурсов, угроз, уязвимостей и нарушителя перед разработкой контрмер, перекрывающих выявленные угрозы, и предпринимаемых для нейтрализации уязвимостей, делающих возможной реализацию этих угроз.

Формирование и уточнение требований по защите информации связано не только с конкретизацией самих требований, но и с заданием классов (уровней) защищенности, если изначально эти классы не задавались. Классы защищенности определяются в соответствии с нормативными документами того ведомства, в системе которого предполагается аттестация разрабатываемой или совершенствуемой АС – МО РФ, ФСТЭК или ФСБ России. Аттестация, в свою очередь, требует сертификации используемых программно-аппаратных средств в соответствии с заданным классом защищенности.

Таким образом, при выработке контрмер необходимо:

– определить требуемые классы (уровни) защищенности АС и используемых средств;

– описать контрмеры, основанные на использовании рассматриваемых средств защиты, перекрывающих выявленные угрозы, и предпринимаемые для уменьшения уязвимостей, делающих возможной реализацию этих угроз;

– сформировать схему размещения рассматриваемых средств защиты с указанием режимов функционирования и параметров конфигурации, обеспечивающих максимальную степень стойкости защиты;

– определить порядок реализации контрмер и применения рассматриваемых средств защиты;

– сформировать рекомендации по поддержанию принятых контрмер в актуальном состоянии, исключающем рост имеющихся и появление новых уязвимостей.

Действуют следующие руководящие документы ФСТЭК России (ранее – Гостехкомиссии) по классификации АС, средств вычислительной техники (СВТ), межсетевых экранов (МЭ) и программного обеспечения (ПО):

– РД. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. – Гостехкомиссия России, 1992 (РД АС).

– РД. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. – Гостехкомиссия России, 1992 (РД СВТ).

– РД. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. – Гостехкомиссия России. – 1997 (РД МЭ).

– РД. Защита от несанкционированного доступа к информации. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. – Гостехкомиссия России, 1999 (РД НДВ).

Концепция защиты СВТ и АС от НСД к информации предусматривает существование двух относительно самостоятельных и, следовательно, имеющих отличие направлений в проблеме защиты информации от несанкционированного доступа (НСД). Это - направление, связанное с СВТ, и направление, связанное с АС:

– 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.

– При создании АС появляются такие отсутствующие при разработке СВТ характеристики АС, как полномочия пользователей, модель нарушителя, технология обработки информации.

– Защита СВТ обеспечивается комплексом программно-технических средств.

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

В соответствии с РД АС устанавливается девять классов защищенности АС от несанкционированного доступа к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС. Класс, соответствующий высшей степени защищенности для данной группы, обозначается индексом NA, где N – номер группы от 1 до 3. Следующий класс обозначается NБ и т.д.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Данная группа содержит два класса 3Б и 3А. Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности. Эта группа содержит два класса 2Б и 2А. Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Данная группа содержит пять классов 1Д, 1Г, 1В, 1Б и 1А. Требования к подсистемам защиты для каждого класса АС приведены в таблице ниже.

Таблица 1 – Требования к АС по классам защищенности

| *Подсистемы и требования* | *Классы* | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | *3Б* | *3А* | *2Б* | *2А* | *1Д* | *1Г* | *1В* | *1Б* | *1А* |
| **I. Подсистема управления доступом** |  |  |  |  |  |  |  |  |  |
| * 1. **Идентификация, проверка подлинности и контроль доступа субъектов:** |  |  |  |  |  |  |  |  |  |
| * в систему | **+** | **+** | **+** | **+** | **+** | **+** | **+** | **+** | **+** |
| * к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ |  |  |  | **+** |  | **+** | **+** | **+** | **+** |
| * к программам |  |  |  | **+** |  | **+** | **+** | **+** | **+** |
| * к томам, каталогам, файлам, записям, полям записей |  |  |  | **+** |  | **+** | **+** | **+** | **+** |
| * 1. **Управление потоками информации** |  |  |  | **+** |  |  | **+** | **+** | **+** |
| **II. Подсистема регистрации и учета** |  |  |  |  |  |  |  |  |  |
| * 1. **Регистрация и учет** |  |  |  |  |  |  |  |  |  |
| * входа/выхода субъектов доступа в/из системы (узла сети) | **+** | **+** | **+** | **+** | **+** | **+** | **+** | **+** | **+** |
| * выдачи печатных (графических) выходных документов |  | **+** |  | **+** |  | **+** | **+** | **+** | **+** |
| * запуска/завершения программ и процессов (заданий, задач) |  |  |  | **+** |  | **+** | **+** | **+** | **+** |
| * доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи |  |  |  | **+** |  | **+** | **+** | **+** | **+** |
| * доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей |  |  |  | **+** |  | **+** | **+** | **+** | **+** |
| * изменения полномочий субъектов доступа |  |  |  |  |  |  | **+** | **+** | **+** |
| * создаваемых защищаемых объектов доступа |  |  |  | **+** |  |  | **+** | **+** | **+** |
| * 1. **Учет носителей информации** | **+** | **+** | **+** | **+** | **+** | **+** | **+** | **+** | **+** |
| * 1. **Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей** |  | **+** |  | **+** |  | **+** | **+** | **+** | **+** |
| * 1. **Сигнализация попыток нарушения защиты** |  |  |  |  |  |  | **+** | **+** | **+** |
| **III. Криптографическая подсистема** |  |  |  |  |  |  |  |  |  |
| * 1. **Шифрование конфиденциальной информации** |  |  |  | **+** |  |  |  | **+** | **+** |
| * 1. **Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах** |  |  |  |  |  |  |  |  | **+** |
| **IV. Подсистема обеспечения целостности** |  |  |  |  |  |  |  |  |  |
| * 1. **Обеспечение целостности программных средств и обрабатываемой информации** | **+** | **+** | **+** | **+** | **+** | **+** | **+** | **+** | **+** |
| * 1. **Физическая охрана средств вычислительной техники и носителей информации** | **+** | **+** | **+** | **+** | **+** | **+** | **+** | **+** | **+** |
| * 1. **Наличие администратора (службы) защиты информации в АС** |  |  |  | **+** |  |  | **+** | **+** | **+** |
| * 1. **Периодическое тестирование СЗИ НСД** | **+** | **+** | **+** | **+** | **+** | **+** | **+** | **+** | **+** |
| * 1. **Наличие средств восстановления СЗИ НСД** | **+** | **+** | **+** | **+** | **+** | **+** | **+** | **+** | **+** |
| * 1. **Использование сертифицированных средств защиты** |  | **+** |  | **+** |  |  | **+** | **+** | **+** |

Обозначения: “ + ” - требование к данному классу присутствует.

Требования к криптографической подсистеме, указанные в РД АС, утратили силу и в настоящее время определяются нормативными документами ФСБ России.

В соответствии с нормативными документами автоматизированные системы в зависимости от грифа обрабатываемой информации и условий эксплуатации, должны соответствовать следующим классам защищенности:

– для грифа «ОВ» - классы 1А, 2А или 3А;

– для грифа «СС» - классы 1Б, 2А или 3А;

– для грифа «С» - классы 1В, 2А или 3А;

– для грифа «ДСП» - классы 1Г, 2Б или 3Б.

Кроме того, в АС в зависимости от грифа обрабатываемой информации должны использоваться СВТ и ПО не ниже следующих классов (уровней для ПО) по РД СВТ и РД НДВ:

– для грифа «ОВ» - СВТ 2 класса и ПО 1 уровня контроля на отсутствие недекларированных возможностей (НДВ);

– для грифа «СС» - СВТ 3 класса и ПО 2 уровня контроля на отсутствие НДВ;

– для грифа «С» - СВТ 4 класса и ПО 3 уровня контроля на отсутствие НДВ;

– для грифа «ДСП» - СВТ 5 класса и ПО 4 уровня контроля на отсутствие НДВ.

Классы СВТ, МЭ, а также уровни контроля отсутствия НДВ для ПО вводятся документами РД СВТ, РД МЭ и РД НДВ соответственно.

На основе общесистемных требований, тенденций в развитии компьютерных сетей и с учетом недостатков современных компьютерных технологий выработаны технические требования к системе информационно-компьютерной безопасности (Рисунок 1), соблюдение которых позволяет достигнуть требуемой степени защиты информации. По своим техническим возможностям система информационно-компьютерной безопасности должна:

– обеспечивать эффективное выполнение всех приоритетных функций защиты, без которых невозможно достичь требуемой степени защищенности;

– позволять проводить обновления общесистемного ПО с целью устранения имеющихся ошибок, т.е. обеспечивать сохранение функциональности ПО при установке различных Service Pack-ов, Support Pack-ов и прочих «заплаток» от фирм-изготовителей;

– обладать эффективной службой централизованного управления пользователями и ресурсами компьютерной сети или быть полностью интегрированной с полноценной службой каталогов, поставляемой другим разработчиком;

– обеспечивать поэтапное внедрение без нарушения полной работоспособности защищаемой системы и целенаправленную адаптацию при изменении структуры, технологических схем или условий функционирования компьютерной сети;

– обеспечивать возможность динамического и статического контроля защищенности, обнаружения атак в режиме реального времени;

– просто и удобно устанавливаться (инсталлироваться), использоваться и сопровождаться.

К сожалению, в настоящий момент на рынке технических систем информационной безопасности нет продуктов, полностью соответствующих всем перечисленным условиям. Высокие функциональные, эксплуатационные и нормативные требования не позволяют в рамках одного продукта реализовать все необходимые возможности. Поэтому наиболее эффективны решения в области системной интеграции, позволяющие в рамках комплексного подхода к решению проблемы информационно-компьютерной безопасности создавать защищенные автоматизированные системы на основе различных классов средств защиты.

Оптимальный выбор технических методов и средств, необходимых и достаточных для достижения требуемой степени защиты информации, осуществляется на основе тщательного анализа их технико-экономических характеристик. Высокая степень информационно-компьютерной безопасности достигается только в случае объединения используемых для этой цели технических методов и средств в единую систему комплексной защиты, которая должна быть функционально самостоятельной системой.

## Классификация средств вычислительной техники по защищенности от несанкционированного доступа к информации

Гостехкомиссии России (сейчас – ФСТЭК) разделила понятия автоматизированной системы (АС) и средств вычислительной техники (СВТ). Выделение СВТ в отдельную категорию обусловлено тем, что СВТ представляют собой компоненты при построении АС, то есть если СВТ не интегрированы в АС, и не решают какой-то прикладной задачи, то они не содержат пользовательской информации. Помимо этого, АС является более широким понятием, включающим в себя персонал, помещения, технологии обработки информации, учетные записи и полномочия пользователей системы.

Например, персональный компьютер с установленной на него операционной системой формально является СВТ. Но если его поставить в конкретную комнату, закрепить за ним пользователя, выполняющего какую-то работу, – АС. Следует отметить, что средства защиты информации также относятся к СВТ.

СВТ - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

СВТ по защищенности классифицируются в соответствии с Руководящим документом Гостехкомиссиии России (сейчас – ФСТЭК) «Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации» (Гостехкомиссия России, 1992).

Данный руководящий документ устанавливает классификацию средств вычислительной техники по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

Устанавливаются 7 классов защищенности СВТ от НСД к информации, при этом самый низкий класс – седьмой, самый высокий – первый. Каждый класс разбит на 4 группы:

– I группа. 7 класс – СВТ, которые были представлены к оценке, однако не удовлетворяют требованиям более высоких классов.

– II группа. 6 и 5 классы – дискреционная защита.

– III группа. 4, 3 и 2 классы – мандатная защита.

– IV группа. 1 класс – верифицированная защита.

Требования ужесточаются с уменьшением номера класса.

Классы являются иерархически упорядоченными: каждый последующий класс содержит требования всех предыдущих.

В общем случае требования предъявляются к следующим показателям защищенности:

– Дискреционный принцип контроля доступа.

– Мандатный принцип контроля доступа.

– Очистка памяти.

– Изоляция модулей.

– Маркировка документов.

Перечень показателей по классам защищенности СВТ приведен в таблице ниже (Таблица 4). Принятые обозначения:

"-" – нет требований к данному классу;

"+" – новые или дополнительные требования,

"=" – требования совпадают с требованиями к СВТ предыдущего класса.

Таблица 2 – Распределение показателей защищенности по классам средств вычислительной техники

| *Наименование показателя* | *Класс защищенности* | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
|  | *6* | *5* | *4* | *3* | *2* | *1* |
| Дискреционный принцип контроля доступа | + | + | + | = | + | = |
| Мандатный принцип контроля доступа | - | - | + | = | = | = |
| Очистка памяти | - | + | + | + | = | = |
| Изоляция модулей | - | - | + | = | + | = |
| Маркировка документов | - | - | + | = | = | = |
| Защита ввода и вывода на отчужденный носитель информации | - | - | + | = | = | = |
| Сопоставление пользователя с устройством | - | - | + | = | = | = |
| Идентификация и аутентификация | + | = | + | = | = | = |
| Гарантии проектирования | - | + | + | + | + | + |
| Регистрация | - | + | + | + | = | = |
| Взаимодействие пользователя с КСЗ | - | - | - | + | = | = |
| Надежное восстановление | - | - | - | + | = | = |
| Целостность КСЗ | - | + | + | + | = | = |
| Контроль модификации | - | - | - | - | + | = |
| Контроль дистрибуции | - | - | - | - | + | = |
| Гарантии архитектуры | - | - | - | - | - | + |
| Тестирование | + | + | + | + | + | = |
| Руководство пользователя | + | = | = | = | = | = |
| Руководство по КСЗ | + | + | = | + | + | = |
| Тестовая документация | + | + | + | + | + | = |
| Конструкторская (проектная) документация | + | + | + | + | + | + |

Выбор класса защищенности СВТ для автоматизированных систем, создаваемых на базе защищенных СВТ, зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы.

Для всех классов СВТ необходима реализация дискреционного контроля доступа. Дискреционный принцип разграничения доступа предполагает назначение каждому объекту списка контроля доступа, элементы которого определяют права доступа к объекту конкретных пользователей или групп. Эта модель отличается простотой реализации, но ее недостатком является отсутствие механизмов слежения за безопасностью потоков информации. Это означает, что права на доступ к объекту проверяются только при первом обращении к объекту. При этом возникает опасность переноса информации из защищенного объекта в незащищенный (открытый). Более того, субъект с определенным правом доступа может передать это право любому другому субъекту. Для каждой пары субъект-объект должно быть задано явное перечисление допустимых типов доступа (читать, писать и т.д.), которые являются санкционированными для данного субъекта (пользователя или группы пользователей) к данному ресурсу (объекту). Возможны, по меньшей мере, два подхода к построению дискреционного управления доступом:

– каждый объект системы имеет привязанного к нему субъекта, называемого владельцем; именно владелец устанавливает права доступа к объекту;

– система имеет одного выделенного субъекта – суперпользователя, который имеет право устанавливать права владения для всех остальных субъектов системы.

Возможны и смешанные варианты построения, когда одновременно в системе присутствуют как владельцы, устанавливающие права доступа к своим объектам, так и суперпользователь (администратор), имеющий возможность изменения прав для любого объекта и/или изменения его владельца. Именно такой смешанный вариант реализован в большинстве операционных систем (Windows или Linux).

Дискреционное управление доступом является основной реализацией разграничительной политики доступа к ресурсам при обработке конфиденциальных сведений согласно требованиям к системе защиты информации.

Мандатный принцип разграничения доступа (англ. Mandatory access control или MAC) предполагает назначение объекту грифа секретности, а субъекту – уровня допуска. Доступ субъектов к объектам в мандатной модели определяется на основании правил «не читать выше» и «не записывать ниже». Такая система запрещает пользователю или процессу, обладающему определенным уровнем доверия, получать доступ к информации, процессам или устройствам более защищенного уровня. Тем самым обеспечивается изоляция пользователей и процессов, как известных, так и неизвестных системе (неизвестная программа должна быть максимально лишена доверия, и ee доступ к устройствам и файлам должен ограничиваться сильнее). Это означает, что пользователь не может прочитать информацию из объекта, гриф секретности которого выше, чем его уровень допуска. Также пользователь не может перенести информацию из объекта с большим грифом секретности в объект с меньшим грифом секретности. Использование мандатной модели предотвращает утечку конфиденциальной информации, но снижает производительность компьютерной системы.

Важно отметить, что приведенные требования для каждого класса СВТ являются минимально необходимыми.



Рисунок 1 – Технические требования к системе информационно-компьютерной безопасности систем

Предъявляемые требования к методам и средствам технической защиты можно разбить на следующие категории:

– функциональные — решение требуемой совокупности задач защиты;

– требования по надежности — способности корректно, а также с требуемой полнотой и стойкостью выполнять все предусмотренные функции защиты;

– требования по гибкости — возможности адаптации при изменении структуры, технологических схем и условий функционирования защищаемой автоматизируемой системы, а также способности к поэтапному внедрению;

– эргономические — простоты и удобства установки и конфигурирования, администрирования, эксплуатации, а также минимизации помех пользователям;

– качества документации — наличия всех необходимых эксплуатационных документов, правильности оформления, а также полноты, корректности и непротиворечивости их содержания;

– формальные — наличия необходимых сертификатов, протоколов, актов, а также других документально оформленных подтверждений о присутствии заявленных возможностей;

– экономические — минимизация финансовых и ресурсных затрат.

Вопросы?