“ЗАЩИТА” ТЕЛЕФОННОЙ СВЯЗИ НА ОДНОМ ИЗ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

Что такое ФСТЭК ?

ИСТОРИЧЕСКАЯ СПРАВКА по ФСТЭК

Государственная техническая комиссия СССР (Гостехкомиссия СССР) создана в соответствии с постановлением Правительства СССР **от 18 декабря 1973 года.**

Указом Президента Российской Федерации от **5 января 1992 года № 9** на базе Гостехкомиссии СССР создана **Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия России)** с задачами проведения единой технической политики, организации и контроля работ по защите информации в оборонной, экономической, политической, научно-технической и других сферах деятельности.

В соответствии с Указом Президента Российской Федерации от **9 марта 2004 г.** № 314 "О системе и структуре федеральных органов исполнительной власти" и от 20 мая 2004 г. №649 "Вопросы структуры федеральных органов исполнительной власти" Государственная техническая комиссия при Президенте Российской Федерации преобразована в **Федеральную службу по техническому и экспортному контролю (ФСТЭК России**).

ФСТЭК России является федеральным органом исполнительной власти, осуществляющим межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную или служебную тайну, от ее утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию и по противодействию техническим средствам разведки на территории Российской Федерации.

Директор - Сергей Григоров

Согласно указу Президента N 1085, ФСТЭК России является федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, а также специально уполномоченным органом в области экспортного контроля.

Согласно Указу, у директора есть три заместителя, предельная штатная численность центрального аппарата ФСТЭК установлена в 250 человек, предельная штатная численность территориальных органов службы - 984 сотрудника.

В составе ФСТЭК существует Государственный научно-исследовательский испытательный институт проблем технической защиты информации.

Проведение работ, связанных с использованием сведений, составляющих государственную тайну: на территории Российской Федерации; за рубежом	Федеральная служба безопасности и ее территориальные органы; Служба внешней разведки
Осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны в пределах своей компетенции	Федеральная служба безопасности и ее территориальные органы; Служба внешней разведки; ФСТЭК России
Проведение работ, связанных с созданием средств защиты информации в пределах своей компетенции	Федеральная служба безопасности; Служба внешней разведки; ФСТЭК; Министерство обороны

Госаттестация руководителей

Решением Межведомственной комиссии по защите государственной тайны «О документах по организации и проведению государственной аттестации руководителей предприятий, учреждений и организаций, ответственных за защиту сведений, составляющих государственную тайну», от 13 марта 1996 г. № 3 утверждены методические рекомендации, которые устанавливают, что государственная аттестация руководителей предприятий организуется ФСБ России и ее территориальными органами (на территории России), СВР России (за рубежом), ФСТЭК России (в пределах компетенции), а также министерствами и ведомствами, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, в отношении подведомственных им предприятий.

Продление, переоформление, приостановление лицензии

Продление срока действия лицензии производится в том же порядке, который установлен для ее получения.

Переоформление лицензии производится в порядке, установленном для ее получения

Органы безопасности вправе приостанавливать действие лицензии

а) по инициативе предприятия

б) по инициативе органа безопасности (по результатам проверок)

в) по инициативе иных государственных органов (ФСТЭК России, других министерств и ведомств, руководители которых наделены полномочиями по отнесению к государственной тайне сведений в отношении подведомственных им предприятий

Лицензионные требования и условия

- Документом, устанавливающим требования и порядок аттестации средств обработки конфиденциальной информации, является нормативно-методический документ Гостехкомиссии (ФСТЭК) России «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР – К), утвержденный приказом Гостехкомиссии России от 30.08.2002 № 282

Нормативно-методические документы в области стандартизации и сертификации

ФСТЭК России ведется разработка нескольких общих и специальных технических регламентов в сфере информационных технологий:

-общий технический регламент «Безопасность информационных технологий»;

-общий технический регламент «Требования к средствам и системам безопасности информационных технологий»;

-общий технический регламент «Требования по защите информации, обрабатываемой на объектах информатизации».

Подготовлены предложения по разработке технических регламентов в области защиты информации, составляющей гостайну:

-общий технический регламент «Безопасность информации, составляющей государственную тайну»;

-общий технический регламент «Безопасность техники защиты объектов, как носителей информации, составляющей государственную тайну»;

-специальный технический регламент «Безопасность информации, составляющей гостайну, для информационных и телекоммуникационных технологий»;

-специальный технический регламент «Безопасность информации, составляющей гостайну, для систем управления военного назначения».

ФСТЭК России является федеральным органом исполнительной власти, осуществляющим межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную или служебную тайну, от ее утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию и по противодействию техническим средствам разведки на территории Российской Федерации.

ФСТЭК России и ее управления по федеральным округам входят в состав государственных органов обеспечения безопасности Российской Федерации.

Приказы, распоряжения и указания ФСТЭК России, изданные в пределах ее компетенции, обязательны для исполнения аппаратами федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления, предприятиями, учреждениями и организациями.

ФСТЭК России в своей деятельности руководствуется:

- Конституцией Российской Федерации
- федеральными конституционными законами,
- федеральными законами
- указами и распоряжениями Президента Российской Федерации
- постановлениями и распоряжениями Правительства Российской Федерации
- международными договорами Российской Федерации.

Для получения лицензии необходимо выполнить требования в соответствии с постановлениями правительства РФ № 333 от 15.04.1995, № 504 от 15.08.06, № 532 от 31.08.06, N 957 от 29.12.07. Основными требованиями являются:

- соблюдение требований законодательных и иных нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений (только при работах, связанных с с использованием информации, содержащую государственную тайну);
- наличие в структуре предприятия подразделения по защите государственной тайны и необходимого числа специально подготовленных сотрудников для работы по защите информации, уровень квалификации которых достаточен для обеспечения защиты государственной тайны (только при работах, связанных с использованием информации, содержащую государственную тайну);
- наличие на предприятии средств защиты информации, имеющих сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности (только при работах, связанных с использованием информации, содержащую государственную тайну);
- наличие в штате соискателя лицензии (лицензиата) специалистов, имеющих высшее профессиональное образование в области технической защиты информации либо высшее или среднее профессиональное (техническое) образование и прошедших переподготовку или повышение квалификации по вопросам технической защиты информации;
- наличие у соискателя лицензии (лицензиата) помещений для осуществления лицензируемой деятельности, соответствующих техническим нормам и требованиям по технической защите информации, установленным нормативными правовыми актами Российской Федерации, и принадлежащих ему на праве собственности или на ином законном основании;
- наличие на любом законном основании производственного, испытательного и контрольно-измерительного оборудования, прошедшего в соответствии с законодательством Российской Федерации метрологическую поверку (калибровку), маркирование и сертификацию;

- использование автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации, прошедших процедуру оценки соответствия (аттестованных и (или) сертифицированных по требованиям безопасности информации) в соответствии с законодательством Российской Федерации;
- использование предназначенных для осуществления лицензируемой деятельности программ для электронно-вычислительных машин и баз данных на основании договора с их правообладателем;
- наличие нормативных правовых актов, нормативно-методических и методических документов по вопросам технической защиты информации;
- выполнение требований конструкторской, программной и технологической документации, единой системы измерений, системы разработки и запуска в производство средств защиты конфиденциальной информации, а также иных нормативных правовых актов Российской Федерации в области технической защиты информации;
- наличие инженерно-технических работников, имеющих высшее профессиональное образование или прошедшие переподготовку (повышение квалификации) в области информационной безопасности с получением специализации, необходимой для работы с шифровальными (криптографическими) средствами.

Требования руководящих документов Федеральной службы по техническому и экспортному контролю (ФСТЭК) к системе защиты информации от несанкционированного доступа (НСД)

ОСНОВОПОЛАГАЮЩИЕ ДОКУМЕНТЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:

- “Оранжевая КНИГА (TCSEC)”
- Радужная серия
- Гармонизированные критерии Европейских стран (ITSEC)
- Рекомендации X.800
- **Концепция защиты от НСД Гостехкомиссии при Президенте РФ (ФСТЭК с 2004 г.)**

Критерии оценки надежных компьютерных систем (“оранжевая книга”)

DOD 5200.28-STD
Supersedes
CSC-STD-001-83, dtd 15 Aug 83
Library No. S225,711

DEPARTMENT OF DEFENSE STANDARD

DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

DECEMBER 1985

ASSISTANT SECURITY OF DEFENSE
COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE

DoD 5200.28-STD

December 26, 1985

FOREWORD

This publication, DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria," is issued under the authority of an in accordance with DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems," and in furtherance of responsibilities assigned by DoD Directive 5215.1, "Computer Security Evaluation Center." Its purpose is to provide technical hardware/firmware/software security criteria and associated technical evaluation methodologies in support of the overall ADP system security policy, evaluation and approval/accreditation responsibilities promulgated by DoD Directive 5200.28.

Оранжевая книга («Критерии оценки доверенных компьютерных систем» - стандарт министерства обороны США).

- Стандарт был принят в 1983 году. Для адаптации стандарта изменяющимся аппаратно-программным условиям в последствие было принято большое количество сопутствующих документов, приспосабливающих стандарт современным условиям. В Оранжевой книге безопасная компьютерная система - это система, поддерживающая управление доступом к обрабатываемой в ней информации так, что только соответствующим образом авторизованные пользователи или процессы, действующие от их имени, получают возможность читать, писать, создавать и удалять информацию. В оранжевой книге предложены три критерия требований безопасности – политика безопасности, аудит и корректность и сформулированы шесть базовых требований безопасности:
  - *Политика безопасности.* Система должна поддерживать точно определенную политику безопасности.
  - *Метки.* С объектами должны быть ассоциированы метки безопасности, используемые в качестве атрибутов контроля доступа.
  - *Идентификация и аутентификаци*я. Все субъекты должны иметь уникальные идентификаторы.
  - *Регистрация и учет*. Все события, значимые с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном журнале.
  - *Контроль корректности*. Средства защиты должны иметь независимые аппаратные и программные компоненты, обеспечивающие работоспособность функций защиты.
  - *Непрерывность защиты*. Все средства защиты должны быть защищены от несанкционированного вмешательства.
- В Оранжевой книге определяются четыре уровня доверия: D, C, B и A. Уровень D соответствует системам, признанным неудовлетворительными с точки зрения безопасности. По мере продвижения от уровня C к уровню A к системе предъявляются все более жесткие требования. Уровни C и B подразделяются также на классы, с постепенным возрастанием степени доверия. Всего имеется шесть таких классов (вместе с уровнем A): C1, C2, B1, B2, B3, A.

Документы по информационной безопасности Национального центра компьютерной безопасности США и Министерства обороны США (“Радужная серия”)

- Светло-коричневая книгаNCSC-TG-001A Guide to Understanding Audit in Trusted SystemsЯрко-синяя книгаNCSC-TG-002Trusted Product Evaluation - A Guide for VendorsОранжевая книгаNCSC-TG-003A Guide to Understanding Discretionary Access Control in Trusted SystemsСине-зеленая книгаNCSC-TG-004Glossary of Computer Security TermsКрасная книгаNCSC-TG-005Trusted Network InterpretationЯнтарная книгаNCSC-TG-006A Guide to Understanding Configuration management in Trusted SystemsБордовая книгаNCSC-TG-007A Guide to Understanding Design Documentation in Trusted SystemsЛиловая книгаNCSC-TG-008A Guide to Understanding Trusted Distribution in Trusted SystemsСеро-зеленая книгаNCSC-TG-009Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation CriteriaГолубая книгаNCSC-TG-010A Guide to Understanding Security Modeling in Trusted SystemsКрасная книгаNCSC-TG-011Trusted Network Interpretation Environments Guideline - Guidance for Applying the Trusted Network Interpretation Розовая книгаNCSC-TG-013Rating Maintenance Phase Program DocumentТемно-фиолетовая книгаNCSC-TG-014Guidelines for Formal Verification SystemsКоричневая книгаNCSC-TG-015A Guide to Understanding Trusted Facility ManagementСалатовая книгаNCSC-TG-016Writing Trusted Facility ManualsБледно-голубая книгаNCSC-TG-017A Guide to Understanding Identification and Authentication in Trusted SystemsБледно-голубая книгаNCSC-TG-018A Guide to Understanding Object Reuse in Trusted SystemsСиняя книгаNCSC-TG-019Trusted Product Evaluation QuestionnaireСерая книгаNCSC-TG-020ATrusted UNIX Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the UNIX SystemТемно-фиолетовая книгаNCSC-TG-021Trusted Database Management System Interpretation of the TCSEC (TDI)Желтая книгаNCSC-TG-022A Guide to Understanding Trusted Recovery in Trusted SystemsЯрко-оранжевая книгаNCSC-TG-023A Guide to Understanding Security Testing and Test Documentation in Trusted SystemsТемно-зеленая книгаNCSC-TG-025A Guide to Understanding Data Remanence in Automated Information SystemsАбрикосовая книгаNCSC-TG-026A Guide to Writing the Security Features User's Guide for Trusted SystemsБирюзовая книгаNCSC-TG-027A Guide to Understanding Information System Security Officer Responsibilities for Automated Information SystemsФиолетовая книгаNCSC-TG-028Assessing Controlled Access ProtectionСиняя книгаNCSC-TG-029Introduction to Certification and Accreditation ConceptsБледно-розовая книгаNCSC-TG-030A Guide to Understanding Covert Channel Analysis of Trusted Systems

Рекомендации X.800.

- Данный документ является основополагающим в области защиты распределенных систем (*см. Глава 7*). В документе перечислены основные функции (сервисы) безопасности, характерные для распределенных систем и роли, которые они могут играть:
  - Аутентификация - обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных.
  - Управление доступом - обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.
  - Конфиденциальность данных - обеспечивает защиту от несанкционированного получения информации.
  - Целостность данных - подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры - с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.
  - *Неотказуемость* (невозможность отказаться от совершенных действий) - обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки. Побочным продуктом неотказуемости является аутентификация источника данных.
- Кроме того, в документе X.800 указан перечень основных механизмов, с помощью которых можно реализовать перечисленные сервисы.

Гармонизированные критерии европейских стран.

- Одна из версий данного стандарта была опубликована в 1991 году от имени Франции, Нидерландов, Германии и Великобритании.
- Стандарт рассматривает основные составляющие информационной безопасности: доступность, целостность, конфиденциальность. В стандарте различается система и продукт.
- Система - это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении.
- Продукт - это аппаратно-программный «пакет», который можно купить и по своему усмотрению встроить в ту или иную систему.
- Таким образом, если система находится в конкретных условиях (окружении), то продукт предназначен для эксплуатации в различных условиях. В стандарте вводится понятие *гарантированности средств защиты*.
- Гарантированность включает в себя эффективность, отражающую соответствие средств безопасности решаемым задачам и корректность, характеризующую процесс разработки и функционирования. При проверке эффективности анализируется соответствие между целями, сформулированными для объекта оценки, и имеющимся набором функций безопасности. Точнее говоря, рассматриваются вопросы адекватности функциональности, взаимной согласованности функций, простоты их использования, а также возможные последствия эксплуатации известных слабых мест защиты. Кроме того, в понятие эффективности входит способность механизмов защиты противостоять прямым атакам (мощность механизма). Определяются три градации мощности - базовая, средняя и высокая.
- Под корректностью понимается правильность реализации функций и механизмов безопасности. В европейском стандарте определяется семь возможных уровней гарантированности корректности - от E0 до E6 (в порядке возрастания). Уровень E0 означает отсутствие гарантированности. При проверке корректности анализируется весь жизненный цикл объекта оценки - от проектирования до эксплуатации и сопровождения.

Руководящие документы Гостехкомиссия при Президенте РФ по проблеме защиты от несанкционированного доступа [1-5] (1992 г.)

[1] Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации. - Москва, 1992.

[2] Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. - Москва, 1992.

[3] Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. - Москва, 1992.

[4] Гостехкомиссия России. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники. - Москва, 1992.

[5] Гостпехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. - Москва, 1992.

Руководящие документы Гостехкомиссии России.

- Данные документы были опубликованы в 1992 году. Всего было пять руководящих документов, посвященных вопросам защиты от несанкционированного доступа к информации. Основным документом является «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». В документе выделяются следующие принципы защиты:
  - **Защита автоматизированных систем обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.**
  - **Защита должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.**
  - **Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики системы.**
  - **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.**
  - **Защита автоматизированных систем должна предусматривать контроль эффективности средств защиты. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем автоматизированной системы или контролирующим органом.**

Руководящие документы Гостехкомиссии России.

В указанных документах предлагается разбить все автоматизированные системы **на девять классов**, по уровню защищенности от несанкционированного доступа к информации.

Каждый класс характеризуется определенной совокупностью требований к средствам защиты. Классы подразделяются на три группы, отличающиеся спецификой обработки информации в системе. Группы определяются на основе следующих признаков:

Наличие в системе различного уровня конфиденциальной информации.

Уровень полномочий пользователя на доступ к конфиденциальной информации.

Режим обработки данных (коллективный или индивидуальный).

ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ РФ

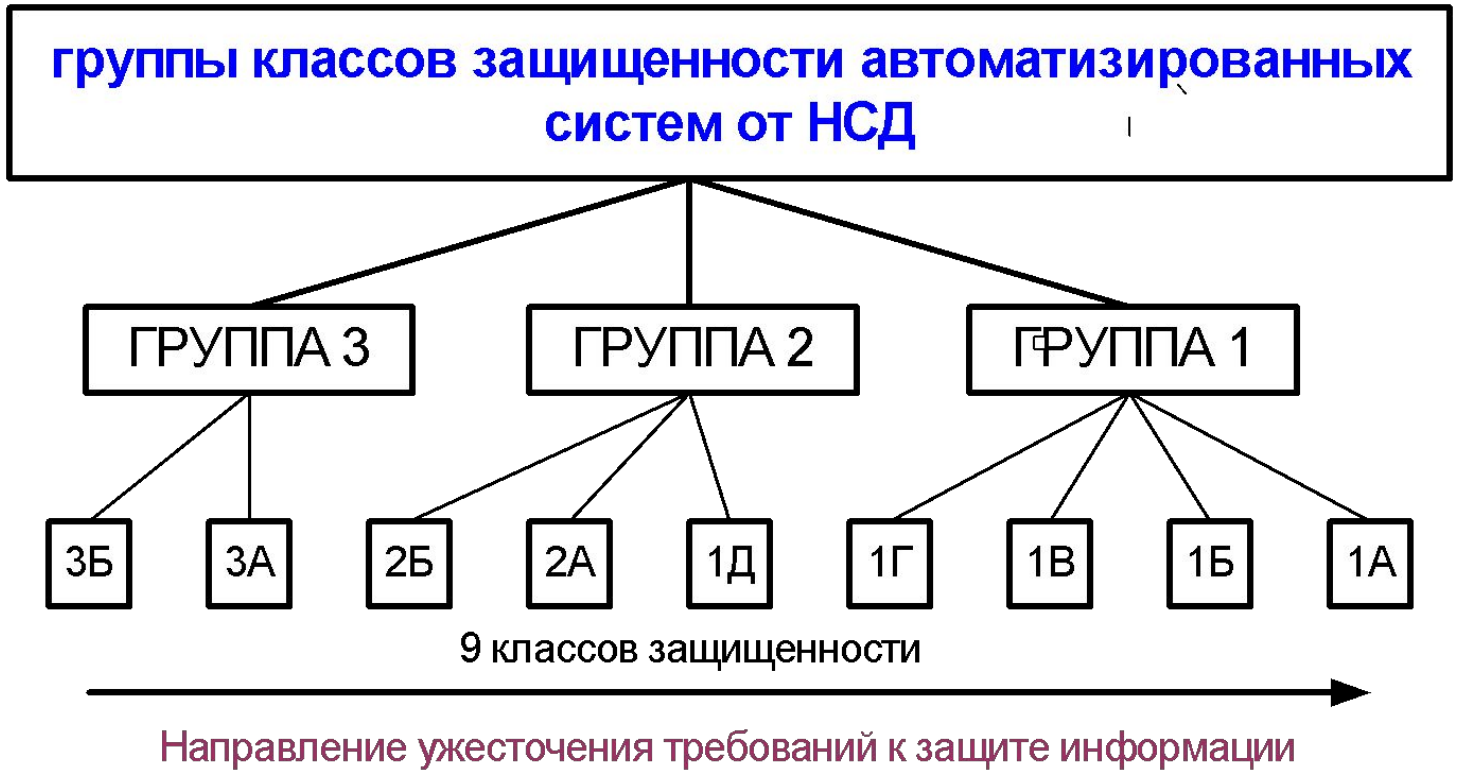
Представлены в руководящем документе (РД) Гостехкомиссии при президенте РФ “Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации” (1992 г.) для государственных и коммерческих организаций, обрабатывающих информацию, содержащую гос.тайну. Для остальных организаций РД носят рекомендательный характер

Руководящий документ разработан в дополнение ГОСТ 24.104-85.

Документ может использоваться как нормативно-методический материал для заказчиков и разработчиков АС при формулировании и реализации требований по защите.

КЛАССИФИКАЦИЯ УРОВНЕЙ ЗАЩИЩЕННОСТИ

АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОТ НСД



КЛАССИФИКАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ

1.1. Классификация распространяется на все действующие и проектируемые
АС учреждений, организаций и предприятий, обрабатывающие конфиденциальную
информацию.
1.2. Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня
защиты информации.
1.3. Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, различием АС по своему
составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала.
1.4. Основными этапами классификации АС являются:
разработка и анализ исходных данных;
выявление основных признаков АС, необходимых для классификации;
сравнение выявленных признаков АС с классифицируемыми;
присвоение АС соответствующего класса защиты информации от НСД.

1.5. Необходимыми исходными данными для проведения классификации
конкретной АС являются:
перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;
перечень лиц, имеющих доступ к штатным средствам АС, с указанием их
уровня полномочий;
матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;
режим обработки данных в АС.

1.6. Выбор класса АС производится заказчиком и разработчиком с привлечением специалистов по защите информации.

1.7. К числу определяющих признаков, по которым производится группировка
АС в различные классы, относятся:
наличие в АС информации различного уровня конфиденциальности;
уровень полномочий субъектов доступа АС на доступ к конфиденциальной
информации;

режим обработки данных в АС: коллективный или индивидуальный.

1.8. Устанавливается девять классов защищенности АС от НСД 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.

1.9. Третья группа классифицирует АС, в которых работает один пользователь,

допущенный ко всей информации АС, размещенной на носителях одного уровня

конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой

и (или) хранимой на носителях различного уровня конфиденциальности. Группа

содержит два класса-2Б и 2А.

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней

конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

2. ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ НСД ДЛЯ АС

2.1. Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.

2.2. В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем:

- **управления доступом;**
- **регистрации и учета;**
- **криптографической;**
- **обеспечения целостности.**

Подсистемы и требования	Классы				
	1Д	1Г	1В	1Б	1А
1. Подсистема управления доступом					
1.1. 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.	–	+	+	+	+
1.2. Управление потоками информации.	–	–	+	+	+
2. Подсистема регистрации и учета					
2.1. 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.	–	–	+	+	+
2.2. Учет носителей информации.	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.	–	+	+	+	+
2.4. Сигнализация попыток нарушения защиты.	–	–	+	+	+

Подсистемы и требования	Классы				
	1Д	1Г	1В	1Б	1А
3. Криптографическая подсистема					
3.1. Шифрование конфиденциальной информации.	-	-	-	+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах.	-	-	-	-	+
3.3. Использование аттестованных (сертифицированных) криптографических средств.	-	-	-	+	+
4. Подсистема обеспечения целостности					
4.1. Обеспечение целостности программных средств и обрабатываемой информации.	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации.	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АС.	-	-	+	+	+
4.4. Периодическое тестирование СЗИ НСД.	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД.	+	+	+	+	+
4.6. Использование сертифицированных средств защиты.	-	-	+	+	+

Обозначения:
" - " - нет требований к данному классу;
" + " - есть требования к данному классу.

Руководящий документ
Средства вычислительной техники
Защита от несанкционированного доступа к информации
Показатели защищенности от несанкционированного доступа к информации

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

Настоящий Руководящий документ устанавливает классификацию средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

1.4. Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс – седьмой, самый высокий – первый.

Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:
- первая группа содержит только один седьмой класс;
- вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

1.5. 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.**

1.6. Применение в комплекте СВТ средств криптографической защиты информации по ГОСТ 28147-89 может быть использовано для повышения гарантий качества защиты.

2. Требования к показателям защищенности

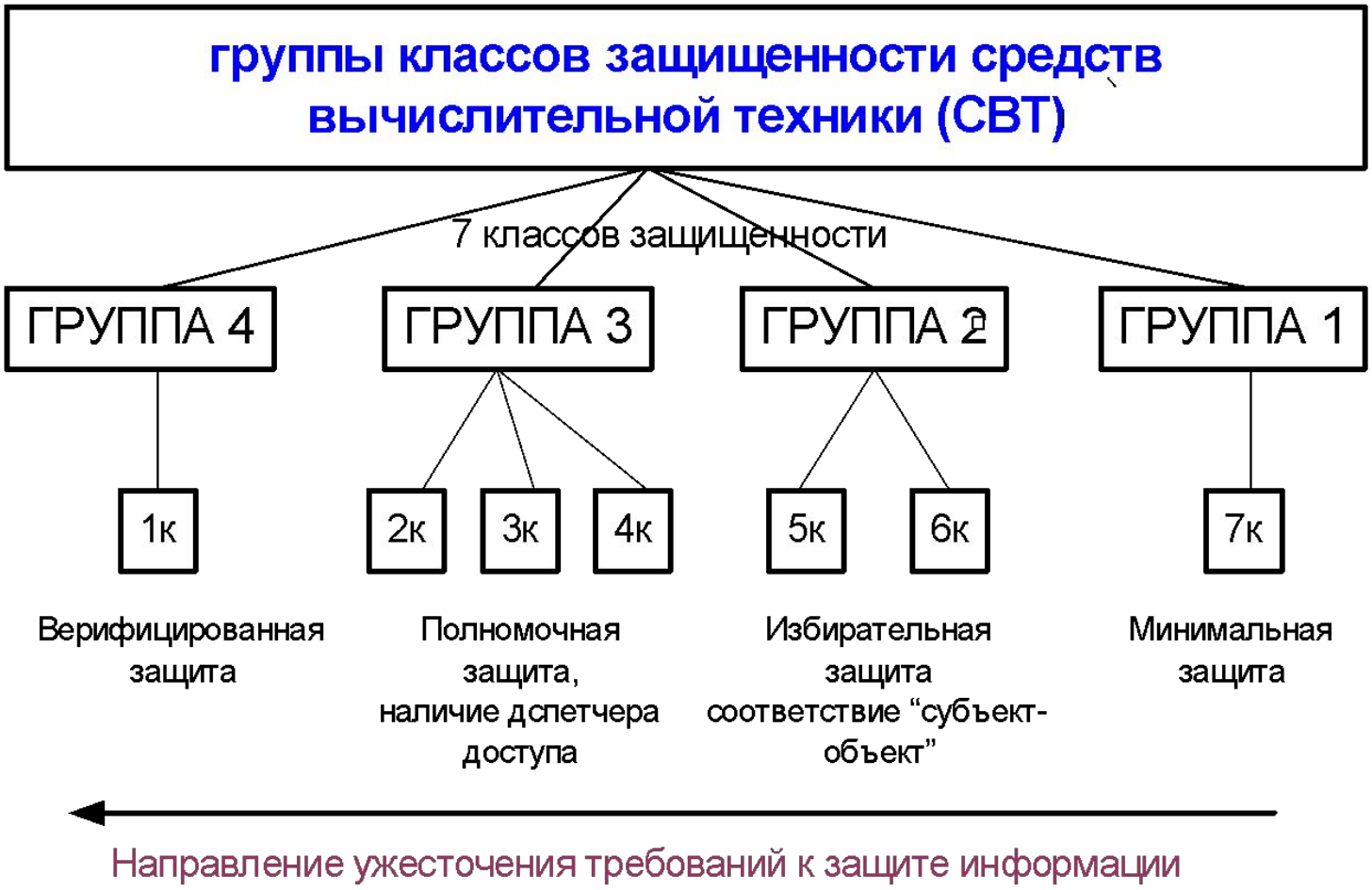
2.1. Показатели защищенности

2.1.1. Перечень показателей по классам защищенности СВТ приведен в таблице.

Обозначения:
- "-" – нет требований к данному классу;
- "+" – новые или дополнительные требования,
- "=" – требования совпадают с требованиями к СВТ предыдущего класса.

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 отчуждаемый физический носитель информации	-	-	+	=	=	=
Сопоставление пользователя с устройством	-	-	+	=	=	=
Идентификация и аутентификация	+	=	+	=	=	=
Гарантии проектирования	-	+	+	+	+	+
Регистрация	-	+	+	+	=	=
Взаимодействие пользователя с КСЗ	-	-	-	+	=	=

КЛАССЫ ЗАЩИЩЕННОСТИ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ОТ НСД



Для присвоения класса защищенности система должна также иметь:

- Руководство администратора по системе
- Руководство пользователя
- Тестовую и конструкторскую документацию

ТРЕБОВАНИЯ ПО ЗАЩИЩЕННОСТИ СВТ ОТ НСД

Наименование показателя	Класс защищенности					
	6	5	4	3	2	1
1. Дискреционный принцип контроля доступа	+	+	+	=	+	=
2. Мандатный принцип контроля доступа	-	-	+	=	=	=
3. Очистка памяти	-	+	+	+	=	=
4. Изоляция модулей	-	-	+	=	+	=
5. Маркировка документов	-	-	+	=	=	=
6. Защита ввода и вывода на отчуждаемый физический носитель информации	-	-	+	=	=	=
7. Сопоставление пользователя с устройством	-	-	+	=	=	=
8. Идентификация и аутентификация	+	=	+	=	=	=
9. Гарантии проектирования	-	+	+	+	+	+
10. Регистрация	-	+	+	+	=	=
11. Взаимодействие пользователя с КСЗ	-	-	-	+	=	=
12. Надежное восстановление	-	-	-	+	=	=
13. Целостность КСЗ	-	+	+	+	=	=
14. Контроль модификации	-	-	-	-	+	=
15. Контроль дистрибуции	-	-	-	-	+	=
16. Гарантии архитектуры	-	-	-	-	-	+
17. Тестирование	+	+	+	+	+	=
18. Руководство пользователя	+	=	=	=	=	=
19. Руководство по КСЗ	+	+	=	+	+	=
20. Тестовая документация	+	+	+	+	+	=
21. Конструкторская (проектная) документация	+	+	+	+	+	+