СЗИ - Средства защиты информации - Công cụ bảo mật thông tin

НСД. несанкционированный доступ: truy cập trái phép

ФСТЭК России под системой защиты информации от НСД понимает совокупность мер организационного характера и программно-технических СЗИ от НСД.

NSD. FSTEC của Nga hiểu hệ thống bảo vệ thông tin chống truy cập trái phép là tập hợp các biện pháp tổ chức và hệ thống bảo mật thông tin phần mềm và phần cứng chống truy cập trái phép.

СВТ - средства вычислительной техники: Cơ sở máy tính

АС - автоматизированные системы: hệ thống tự động

НДВ - незадекларированная возможность: khả năng không được khai báo

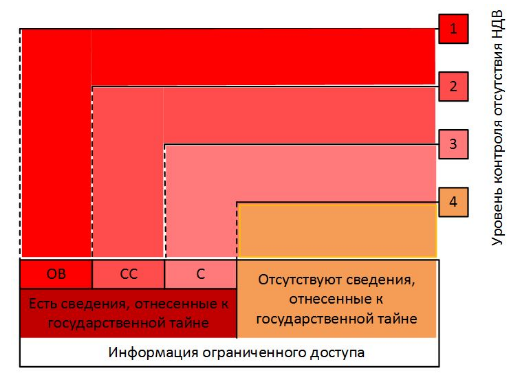
ГИС - государственных информационных системах

АСУ - автоматизированная система управления

ИСПДн - информационная система персональных данных

1. **Классификация по уровню контроля на отсутствие НДВ**

Регулятор выделил 4 уровня контроля отсутствия НДВ: первый — наивысший, а четвертый — низший



Как показано на рисунке 2, если СЗИ предназначено для защиты информации с грифом секретности «особой важности», то оно должно удовлетворять требованиям, предъявляемым к 1 уровню контроля.

Như được hiển thị trong Hình 2, nếu hệ thống bảo mật thông tin nhằm mục đích bảo vệ thông tin được phân loại là “đặc biệt quan trọng” thì hệ thống đó phải đáp ứng các yêu cầu về kiểm soát cấp độ 1.

В случае защиты информации с грифом секретности «совершенно секретно», то программное обеспечение применяемого СЗИ должно пройти как минимум второй уровень контроля.

Trong trường hợp bảo vệ thông tin thuộc loại “tuyệt mật”, phần mềm của hệ thống bảo mật thông tin được sử dụng phải vượt qua ít nhất cấp độ kiểm soát thứ hai.

Если гриф секретности защищаемой информации «секретно», то соответствие требованиям по третьему уровню контроля будет достаточным.

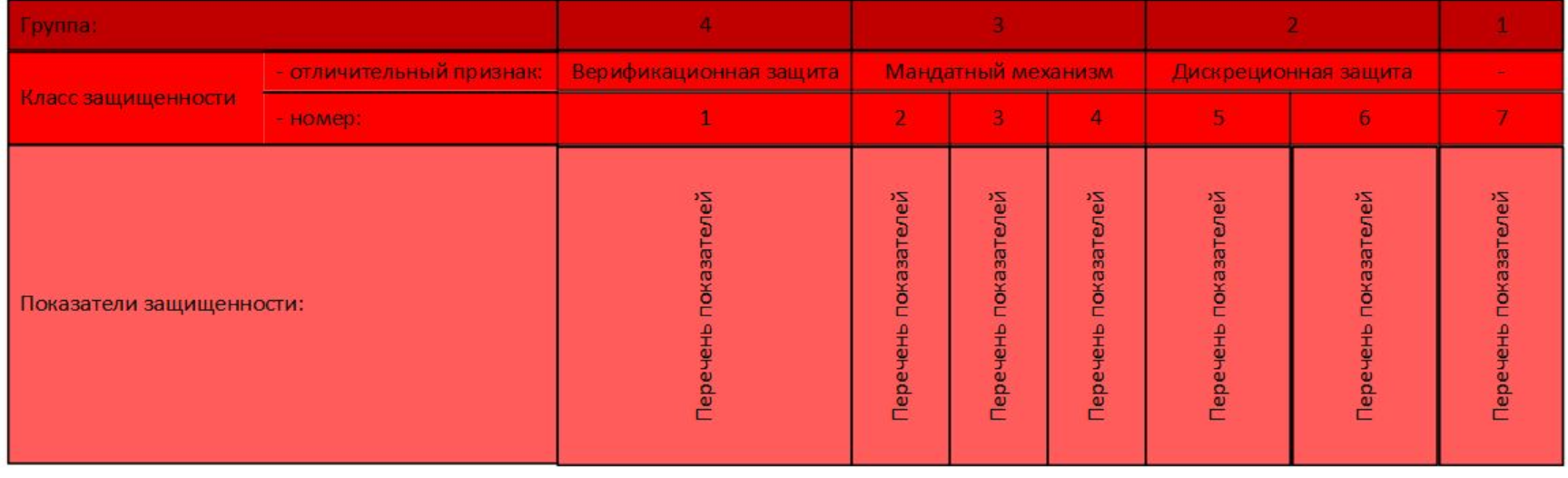
Nếu việc phân loại thông tin được bảo vệ là "bí mật", thì việc tuân thủ các yêu cầu đối với cấp độ kiểm soát thứ ba là đủ.

Что касается информации ограниченного доступа, не содержащей сведений, относящихся к государственной тайне, — достаточным уровнем контроля является самый низкий.

Đối với thông tin bị hạn chế truy cập không chứa thông tin liên quan đến bí mật nhà nước thì mức kiểm soát thấp nhất là đủ.

**2.Классификация защищенности средств вычислительной техники (CBT)**

Phân loại mức độ bảo mật của thiết bị máy tính - có 7 lớp



* Nhóm 1 - Lớp 7:

mức độ bảo mật của nó thấp hơn lớp 6

được thiết lập cho những máy tính phải có cơ chế chống truy cập trái phép - НСД

* Nhóm 2 - Lớp 6, 5:

Они отличаются наличием дискреционного управления доступом. Этот механизм позволяет задавать правила доступа пользователей к различным ресурсам, таким как файл, программа и пр., в которых явно указано, что именно можно делать субъекту: читать содержимое файла, выполнять запуск программы и т. д.

Chúng được phân biệt bởi sự hiện diện của kiểm soát truy cập tùy ý. Cơ chế này cho phép bạn đặt quy tắc để người dùng truy cập vào nhiều tài nguyên khác nhau, chẳng hạn như tệp, chương trình, v.v., trong đó chỉ rõ chính xác những gì chủ thể có thể làm: đọc nội dung của tệp, chạy chương trình, v.v.

* Nhóm 3 - Lớp 4,3,2:

Образующие третью группу 4, 3 и 2 классы отличаются реализацией мандатного управления доступом, основанным на использовании классификационных меток. Они позволяют пользователям и ресурсам назначать т. н. классификационные уровни, например — категории секретности обрабатываемой информации. Так, создается иерархическая структура, в которой пользователь может получить доступ к ресурсу в том случае, если его уровень в созданной иерархии не ниже уровня иерархии требуемого ресурса. В случае иерархической структуры в классификационный уровень пользователя включают те классификационные уровни ресурсов, доступ к которым этому пользователю должен быть обеспечен.

Các lớp 4, 3 và 2, tạo thành nhóm thứ ba, được phân biệt bằng cách thực hiện kiểm soát truy cập bắt buộc dựa trên việc sử dụng nhãn phân loại. Chúng cho phép người dùng và tài nguyên chỉ định cái gọi là. các cấp độ phân loại, ví dụ - các loại bí mật của thông tin được xử lý. Do đó, một cấu trúc phân cấp được tạo trong đó người dùng có thể truy cập tài nguyên nếu cấp độ của anh ta trong hệ thống phân cấp đã tạo không thấp hơn cấp độ phân cấp của tài nguyên được yêu cầu. Trong trường hợp cấu trúc không phân cấp, cấp độ phân loại của người dùng bao gồm các cấp độ phân loại tài nguyên mà người dùng này phải được cấp quyền truy cập.

При этом в этих средствах вычислительной техники присутствует механизм дискреционного управления доступом: дискреционные правила служат дополнением мандатных.

Đồng thời, các cơ sở máy tính này chứa một cơ chế kiểm soát truy cập tùy ý: các quy tắc tùy ý bổ sung cho các quy tắc bắt buộc.

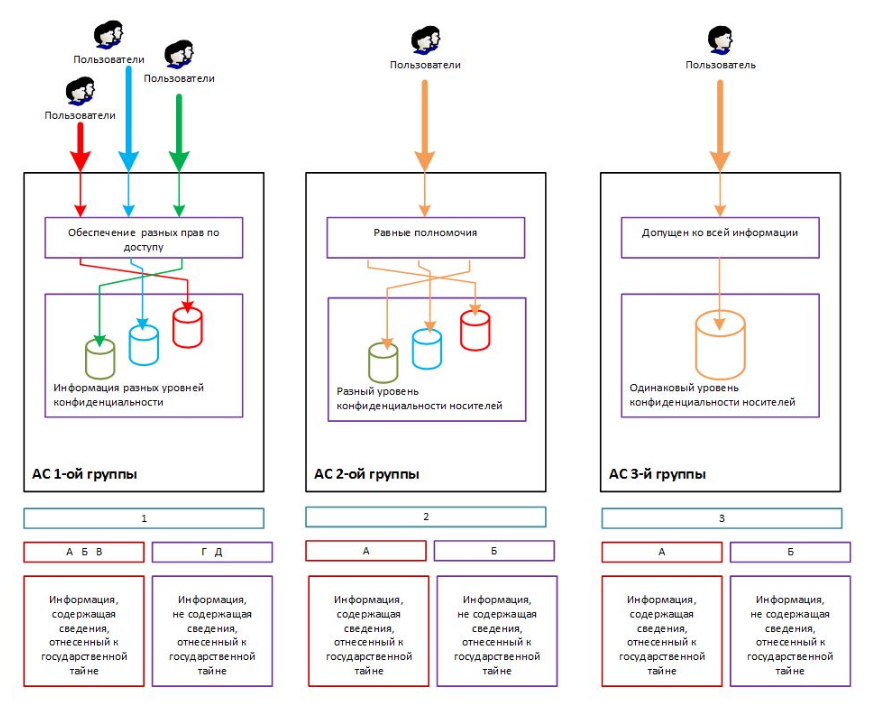
* Nhóm 4 - Lớp 1

А в состав четвертой группы входил только 1 класс, характеризующийся наличием верифицированной защиты. Реализованный механизм защиты должен гарантированно обеспечивать перехват диспетчером доступа всех обращений субъектов доступа к объектам.

Và nhóm thứ tư chỉ bao gồm 1 lớp, được đặc trưng bởi sự hiện diện của khả năng bảo vệ đã được xác minh. Cơ chế bảo vệ được triển khai phải đảm bảo rằng trình quản lý truy cập chặn tất cả các yêu cầu từ chủ thể truy cập đến đối tượng.

1. Классификация средств защиты автоматизированных систем (AC)

Phân loại phương tiện bảo vệ hệ thống tự động



* Классы 1 группы — 1Д, 1Г, 1В, 1Б и 1А. Они характеризуют системы, в которых работает несколько пользователей. Пользователи имеют разные права доступа к информации. Уровни конфиденциальности информации также различны.

**Các lớp thuộc nhóm 1 - 1D, 1G, 1B, 1B và 1A. Chúng mô tả các hệ thống trong đó có nhiều người dùng làm việc. Người dùng có các quyền khác nhau để truy cập thông tin. Mức độ bảo mật thông tin cũng khác nhau.**

* Во 2 группе — классы 2Б и 2А. В системах таких классов у пользователей равные полномочия в отношении всей информации. Сама же информация находится на носителях различного уровня конфиденциальности.

**Ở nhóm 2 - lớp 2B và 2A. Trong các hệ thống lớp học như vậy, người dùng có quyền bình đẳng đối với mọi thông tin. Bản thân thông tin được đặt trên các phương tiện truyền thông có mức độ bảo mật khác nhau.**

* И, наконец, 3 группу образуют классы 3Б и 3А. В этом случае речь идет об однопользовательских системах. Пользователь допущен ко всей информации. Уровень конфиденциальности носителей — одинаковый.

Và cuối cùng, nhóm 3 được thành lập bởi lớp 3B và 3A. Trong trường hợp này chúng ta đang nói về hệ thống một người dùng. Người dùng được phép truy cập vào tất cả các thông tin. Mức độ bảo mật của các phương tiện truyền thông là như nhau.

* Также определено, что если АС работает со сведениями, отнесенными к гостайне, то класс системы не должен быть ниже 3А, 2А, 1А, 1Б или 1В. При этом, для класса защищенности:
* 1В должны применяться средства вычислительной техники не ниже 4 класса;
* 1Б — не ниже 3 класса;
* 1А — не ниже 2 класса.

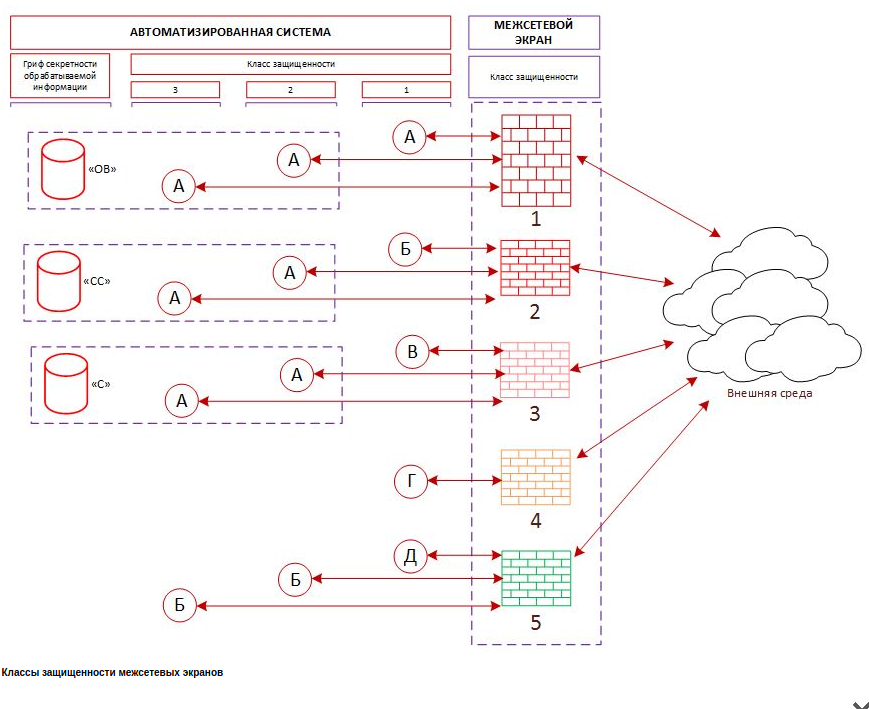
Người ta cũng xác định rằng nếu AS làm việc với thông tin được phân loại là bí mật nhà nước thì cấp của hệ thống không được thấp hơn 3A, 2A, 1A, 1B hoặc 1B. Trong trường hợp này, đối với lớp bảo mật:

Phải sử dụng thiết bị máy tính loại 1B ít nhất là loại 4;

1B - không thấp hơn hạng 3;

1A - không thấp hơn hạng 2.

1. **Классификация межсетевых экранов: Phân loại tường lửa (МЭ)**



Lớp 1

* Самый высокий — 1-й класс. Он применим, когда требуется обеспечить безопасное взаимодействие автоматизированных систем класса 1А с внешней средой.

Cao nhất là hạng 1. Nó được áp dụng khi cần thiết để đảm bảo sự tương tác an toàn giữa các hệ thống tự động loại 1A và môi trường bên ngoài.

* Если в автоматизированных системах классов 3А, 2А обрабатывается информация с грифом «особой важности», то требуется использовать межсетевой экран не ниже 1 класса.

Nếu thông tin được phân loại là “tầm quan trọng đặc biệt” được xử lý trong hệ thống tự động cấp 3A, 2A thì bắt buộc phải sử dụng tường lửa ít nhất là cấp 1.

Lớp 2:

* Для защиты взаимодействия с внешним миром систем класса 1Б предназначены межсетевые экраны 2 класса.

Để bảo vệ sự tương tác với thế giới bên ngoài của hệ thống lớp 1B, tường lửa lớp 2 được thiết kế.

* Если в системах классов 3А, 2А обрабатывается информация с грифом «совершенно секретно», необходимо использовать межсетевые экраны не ниже указанного класса.

Nếu thông tin được phân loại là “tuyệt mật” được xử lý trong các hệ thống cấp 3A, 2A thì cần phải sử dụng tường lửa ít nhất thuộc loại được chỉ định.

Lớp 3:

* Защита взаимодействия систем класса 1В обеспечивается межсетевыми экранами 3 класса. Если в автоматизированных системах классов 3А, 2А происходит обработка информации с грифом «секретно», потребуется межсетевой экран не ниже 3 класса.

Bảo vệ tương tác hệ thống lớp 1B được cung cấp bởi tường lửa lớp 3. Nếu thông tin được phân loại là “bí mật” được xử lý trong hệ thống tự động cấp 3A, 2A thì sẽ cần có tường lửa ít nhất cấp 3

Lớp 4:

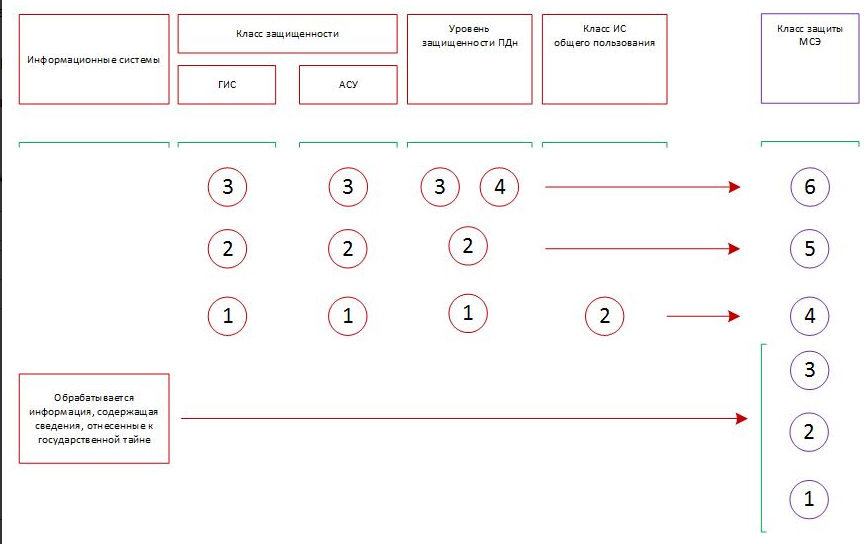
* Межсетевые экраны 4 класса требуются в случае защиты взаимодействия автоматизированных систем класса 1Г с внешней средой.

Tường lửa lớp 4 được yêu cầu để bảo vệ sự tương tác của các hệ thống lớp 1G tự động với môi trường bên ngoài.

Взаимодействие систем класса 1Д должны обеспечивать межсетевые экраны 5 класса. Также требуется использовать их не ниже указанного класса для автоматизированных систем класса 3Б и 2Б.

Sự tương tác của các hệ thống lớp 1D phải được đảm bảo bởi tường lửa lớp 5. Cũng cần phải sử dụng chúng không thấp hơn loại được chỉ định cho các hệ thống tự động loại 3B và 2B.

1. **Классы защиты межсетевых экранов: Các lớp bảo vệ tường lửa**



có 6 lớp

По такому подходу, в информационных системах защита информации, содержащей сведения, отнесенные к государственной тайны, должна обеспечиваться с помощью межсетевых экранов 3, 2 и 1 классов защиты.

Theo cách tiếp cận này, trong các hệ thống thông tin, việc bảo vệ thông tin chứa thông tin được phân loại là bí mật nhà nước cần được đảm bảo bằng cách sử dụng tường lửa cấp bảo vệ 3, 2 và 1.

Что касается остальных случаев, то в государственных информационных системах (ГИС) 1, 2 и 3 классов защиты должны использоваться межсетевые экраны 4, 5 и 6 классов соответственно. Аналогичная ситуация в отношении автоматизированных систем управления производственными и технологическими процессами (далее — АСУ).

Đối với các trường hợp khác, trong hệ thống thông tin chính phủ (GIS) thuộc lớp bảo vệ 1, 2 và 3, nên sử dụng tường lửa thuộc lớp 4, 5 và 6 tương ứng. Tình huống tương tự đối với các hệ thống điều khiển tự động cho các quy trình sản xuất và công nghệ (sau đây gọi tắt là ACS).

Для обеспечения 1 и 2 уровней защищенности персональных данных в информационных системах персональных данных (ИСПДн) потребуется устанавливать межсетевые экраны 4 и 5 классов соответственно. Если же требуется обеспечить 3 или 4 уровень защищенности персональных данных, то достаточно 6 класса защиты.

Để đảm bảo mức độ bảo mật dữ liệu cá nhân cấp 1 và 2 trong hệ thống thông tin dữ liệu cá nhân (PDIS), cần phải cài đặt tường lửa loại 4 và 5 tương ứng. Nếu bạn cần đảm bảo bảo mật dữ liệu cá nhân cấp độ 3 hoặc 4 thì cấp độ bảo vệ 6 là đủ.

Регулятор также определил необходимость использования межсетевых экранов 4 класса для защиты информации в информационных системах общего пользования II класса.

Cơ quan quản lý cũng xác định sự cần thiết phải sử dụng tường lửa loại 4 để bảo vệ thông tin trong hệ thống thông tin công cộng loại II.

1. **Типы межсетевых экранов : Các Loại tường lửa**

Регулятор выделяет межсетевые экраны уровня:

сети (тип «А»);

логических границ сети (тип «Б»);

узла (тип «В»); веб-сервера (тип «Г»);

промышленной сети (тип «Д»).

Cơ quan quản lý xác định tường lửa ở các cấp độ sau:

mạng (loại “A”);

ranh giới mạng logic (loại “B”);

nút (loại “B”); máy chủ web (loại “G”);

mạng công nghiệp (loại “D”).

Межсетевые экраны типа «А» реализуется только в программно-техническом исполнении. «Б», «Г» и «Д» могут быть как в виде программного продукта, так и в ПТИ. Исключительно в виде программного продукта реализуется межсетевые экраны типа «В».

Межсетевые экраны типа «А» устанавливают на физическом периметре информационных систем. Если в них есть несколько физических сегментов, то такой межсетевой экран может устанавливаться между ними

Tường lửa loại “A” chỉ được triển khai trong các phiên bản phần mềm và phần cứng. “B”, “G” và “D” có thể ở dạng sản phẩm phần mềm hoặc ở dạng PTI. Tường lửa loại “B” được bán độc quyền dưới dạng sản phẩm phần mềm.

Tường lửa loại A được cài đặt trên chu vi vật lý của hệ thống thông tin. Nếu chúng có một số phân đoạn vật lý thì có thể cài đặt tường lửa như vậy giữa chúng