Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ

Подготовил студент группы «2КС-22»
Арличенков Р.С

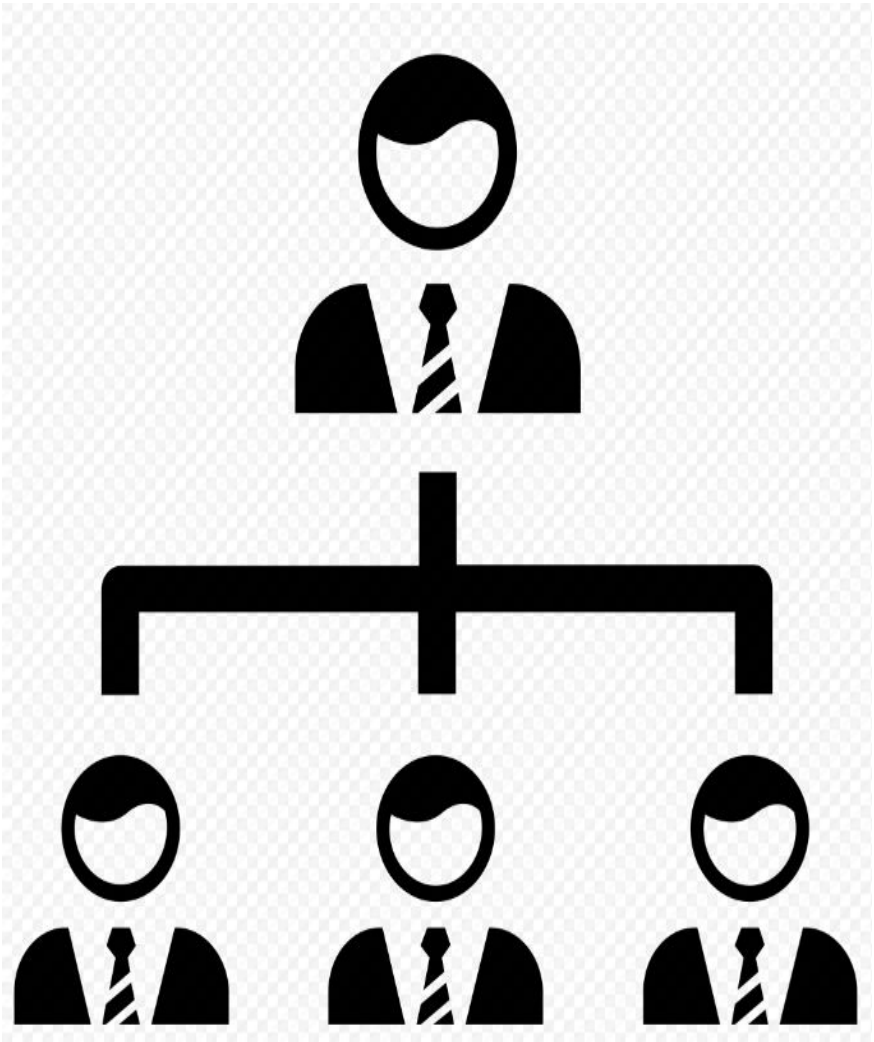
Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ

Информационная безопасность в РФ

- **Структура Гостехкомиссии**
- состоит из центрального аппарата и региональных отделений. Центральный аппарат занимается разработкой стратегии и методологии в области информационной безопасности, а также координацией работы региональных отделений. Региональные отделения осуществляют контроль за соблюдением требований по обеспечению информационной безопасности на территории своего

Задачи и функции Гостехкомиссии
является органом госуправления, осуществляющим координацию и контроль ИБ. Ее задачи включают разработку и принятию мер по защите инф-ции, а также контроль за

Структура Гостехкомиссии



- **Правление Гостехкомиссии**
- Руководитель, осуществляет общее руководство, принимает решения по вопросам, отнесенным к ее компетенции.

Комитеты и рабочие группы
Осуществляют подготовку предложений по вопросам, отнесенным к их компетенции, разрабатывают проекты нормативных документов, проводят научные и экспериментальные работы.

Секретариат Гостехкомиссии
Организация а также подготовка и сопровождение заседаний, в том числе публикацию информации о деятельности комиссии.

Система обеспечения ИБ

Методы и средства защиты информации
Для защиты информации используются различные методы и средства, такие как криптография, аппаратные и программные средства защиты, средства контроля и мониторинга.

- **Структура системы.**
- Система обеспечения информационной безопасности включает в себя комплекс мер и средств, направленных на защиту информации от несанкционированного доступа, использования, изменения, уничтожения, блокирования, копирования и распространения.

Международное сотрудничество

- Гостехкомиссия России активно сотрудничает с международными организациями и странами в области обеспечения ИБ. Мы участвуем в разработке международных стандартов и рекомендаций, обмениваемся опытом и передовыми технологиями,

Оценка угроз ИБ

Методы оценки угроз информационной безопасности

Оценка угроз информационной безопасности может проводиться различными методами, включая:

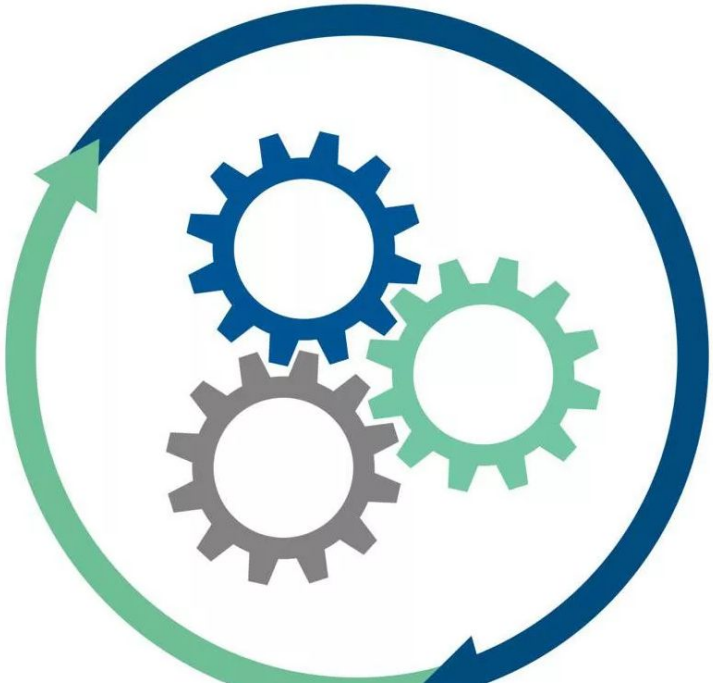
Анализ уязвимостей информационных систем

Экспертные оценки

Моделирование атак и их последствий

- Оценка угроз информационной безопасности является одной из ключевых задач Гостехкомиссии. Это процесс определения потенциальных угроз информационной безопасности, которые могут возникнуть в результате доступа к информации или использования информационных систем.
- Для проведения оценки угроз Гостехкомиссия использует различные методы и инструменты, такие как анализ уязвимостей информационных систем, сбор и анализ статистических данных об инцидентах в области информационной безопасности, а также экспертные оценки.

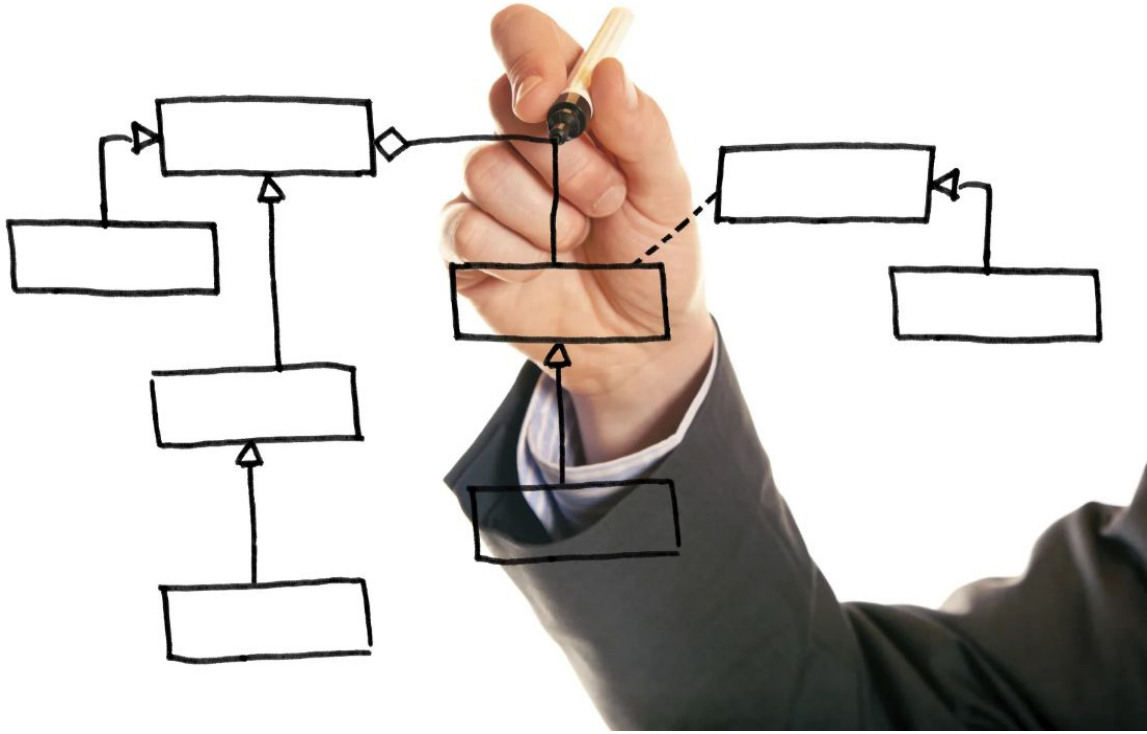
Принципы работы Гостехкомиссии



- Создание и совершенствование ИБ в РФ.
- Разработка и утверждение документов в областиЗИ.
- Оценка угроз ИБ и анализ уязвимостей информационных систем.
- Разработка рекомендаций по обеспечению ИБ и сертификация средств защиты информации.
- Анализ и учет инцидентов в области информационной безопасности.
- Развитие методов и средств ЗИ, включая использование криптографии и средств контроля и мониторинга.

Анализ уязвимостей ИС

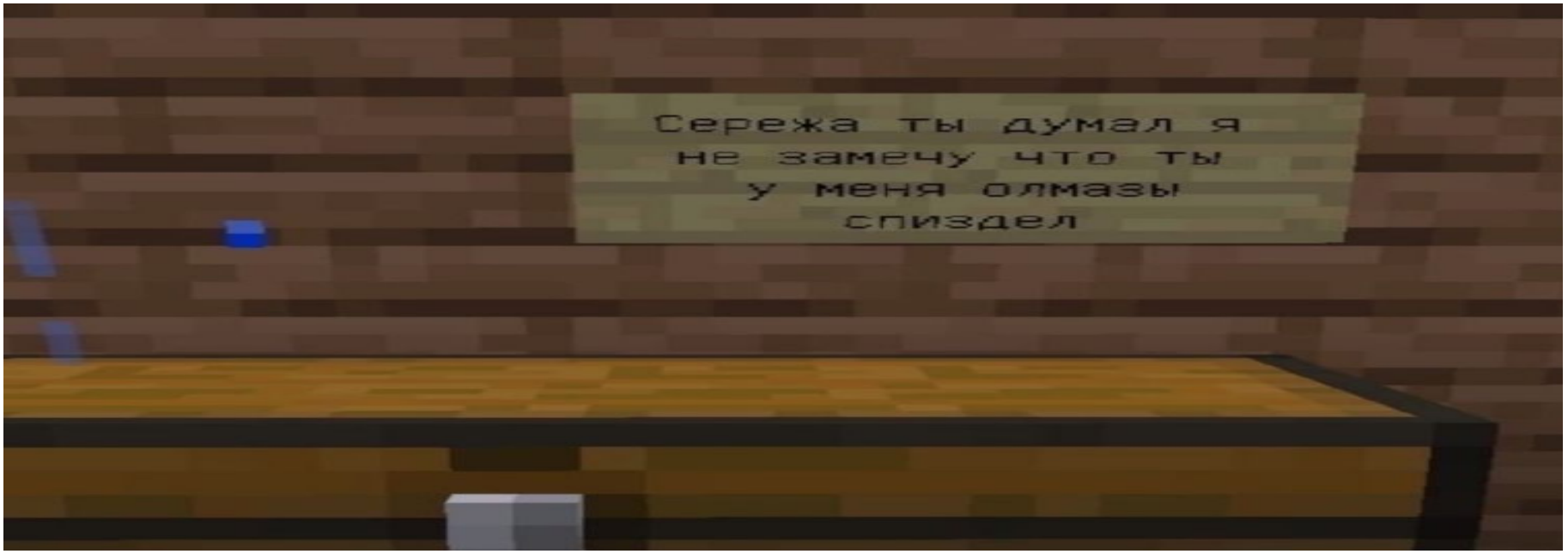
- Анализ уязвимостей может проводиться как в ходе разработки новой ИС, так и при уже существующей.
- При анализе необходимо проводить исследование всех возможных угроз, которые могут возникнуть.
- Необходимо определить вероятность возникновения угроз и их последствия для системы.
- После проведения анализа необходимо принять меры по устранению выявленных проблем.



Разработка рекомендаций по ИБ

- **Общие принципы разработки рекомендаций**
- Разработка рекомендаций по обеспечению ИБ является одним из основных направлений работы Гостехкомиссии. Они разрабатываются на основе анализа угроз и уязвимостей ИС.
- **Содержание рекомендаций**
- Рекомендации по обеспечению ИБ могут содержать рекомендации по выбору и применению средств ЗИ, а также по организации работы с информацией и защите от НСД.

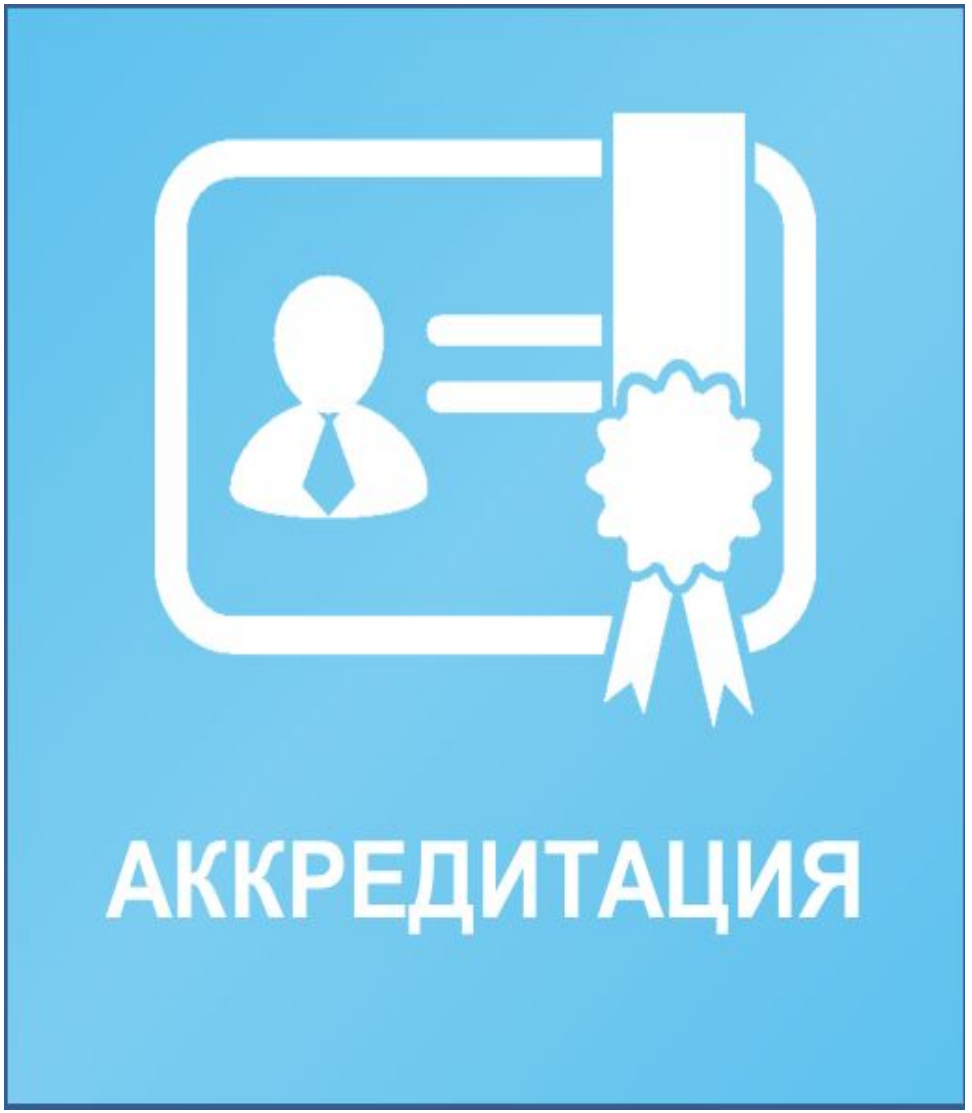
Сертификация средств ЗИ



- Для обеспечения надежной ЗИ в РФ проводится сертификация. Сертификация является процедурой оценки соответствия средств ЗИ требованиям, законодательством РФ.
- Сертификация проводится Гостехкомиссией и включает в себя следующие этапы:
- Подача заявки на сертификацию.
- Проведение испытаний в аккредитованной лаборатории.
- Анализ результатов испытаний и принятие решения о выдаче сертификата.
- Сертификат соответствия является документом, подтверждающим соответствие требованиям и позволяющим его использование в системах, содержащих государственную тайну

Аккредитация организаций по обеспечению ИБ

- **Аккредитация организаций**- Гостехкомиссия осуществляет аккредитацию организаций, занимающихся вопросами ИБ. Аккредитация проводится на основе соответствия организаций установленным требованиям а также сертификации.
- **Процедура аккредитации**- Процедура аккредитации организаций: заявка на аккредитацию, проверку соответствия требованиям, проведение аудита, принятие решения о выдаче или отказе в аккредитации и выдачу свидетельства об аккредитации.
- **Преимущества**-дает возможность повысить качество и эффективность работы в данной области. Аккредитованные организации имеют право проводить работы по оценке и ЗИ , а также сертифицировать средства ЗИ. Кроме того, аккредитация является гарантией для заказчиков, что они получат качественные услуги



Контроль за соблюдением требований

Методы контроля-Контроль за соблюдением требований по обеспечению ИБ осуществляется путем различных методов и инструментов, таких как: мониторинг сетевого трафика, анализ журналов доступа, аудит безопасности, сканирование уязвимостей и др. Все эти методы позволяют выявлять нарушения и принимать меры по их устранению.

Программное обеспечение для контроля-Для контроля за соблюдением требований используются различные ПО, такие как: системы мониторинга и анализа сетевого трафика, системы аудита безопасности, системы сканирования уязвимостей и др. Эти средства позволяют автоматизировать процесс контроля и ускорить выявление нарушений.

Училка в классе

Я жду тишины!

ПАЦАНЫ:

ОБЩАЮТСЯ НА УЛЬТРАЗВУКЕ

У МЕНЯ ЕСТЬ ДУБИНКА

Методы и средств ЗИ

- **Криптография и ее применение в обеспечении информационной безопасности-** Криптография – это наука о методах обеспечения конфиденциальности, и целостности информации. Криптографические методы идут против НСД.
- **Средства защиты информации на основе использования криптографических алгоритмов**- Средства защиты информации на основе криптографических алгоритмов используют шифрование для защиты данных. Они могут включать в себя программное обеспечение, аппаратные устройства и устройства хранения данных.
- **Средства защиты информации на основе использования аппаратных средств**- Средства ЗИ на основе аппаратных средств используются для защиты данных на уровне аппаратного обеспечения. Они могут включать в себя устройства аутентификации, защиту от взлома и защиту от шпионажа.

Средства ЗИ на криптографических алгоритмах

- **Криптография и ее применение в обеспечении информационной безопасности**- Криптография это наука о методах ЗИ от НСД. Криптографические алгоритмы - это математические функции, которые используются для шифрования и дешифрования данных.
- **Применение криптографических алгоритмов в обеспечении информационной безопасности**- Криптографические алгоритмы используются в различных областях, таких как банковское дело, правительственные организации, военные учреждения, медицинские учреждения и т.д. Они могут быть использованы для защиты данных в хранилищах, передачи данных по сетям, аутентификации пользователей и т.д.

Средства ЗИ аппаратных средств

Атолл-3

Гранит-VIII

Корунд-М

МП-1Ц

Antifly

SEC-2000 Ultra

SEC-2004 Antifly

Грань-300

Вьюга-4

SEL SP-41/C

БАРЬЕР-4

СКИТ-М-С

ИМПУЛЬС

МП-3

СОНАТА-С1

SEL SP-41/D

SI-8001

СОПЕРНИК

ЦИКАДА-М1

- **Принципы работы аппаратных средств защиты информации-** Аппаратные средства ЗИ работают на основе алгоритмов шифрования и контроля доступа к информации. Они могут быть реализованы в виде специальных устройств, таких как шифраторы, криптографические процессоры, аппаратные модули безопасности и т.д.
- **Примеры аппаратных средств защиты информации-** Шифраторы и дешифраторы Криптографические процессоры Аппаратные модули безопасности Сетевые экраны Системы управления доступом

Средства ЗИ на основе ПО

KASPERSKY

Dr.WEB®

KATANA

Kills Active Threats and New Attacks

ПО- ПО для ЗИ включает в себя различные виды антивирусных программ, программы защиты от взлома и шпионских программ, программы для мониторинга сетевого трафика и системы обнаружения вторжений.

- **Антивирусное ПО**- ПО предназначено для выявления и удаления вирусов, троянов, руткитов и других вредоносных программ, которые могут причинить вред информационной системе.
- **Программы защиты от взлома и шпионских программ**-предназначены для защиты от НСД и контроля за активностью пользователей на компьютере или в сети. **Программы для мониторинга сетевого трафика**-для контроля за передачей данных в сети и выявления НСД . Они также могут использоваться для оптимизации работы сети и выявления проблем в ее работе.

Средства ЗИ на основе использования средств контроля и мониторинга

- **Средства контроля и мониторинга-** являются одними из наиболее эффективных средств ЗИ . Они позволяют обнаруживать и предотвращать попытки НСД , а также просматривать работу ИС и обнаруживать возможные уязвимости.
- **Принципы работы систем контроля и мониторинга-** постоянный мониторнг ИС, анализ данных и обнаружение угроз, а также предотвращение их реализации. Для этого используются различные методы и средства, включая системы регистрации и анализа событий, системы обнаружения вторжений, системы аудита безопасности и т.д.


ПОСТАВЬТЕ ПЯТЬ ПОЖАЛУЙСТА
ЛДПР
ХВАТИТ ТЕРПЕТЬ ДВОЙКИ!

На этом все!
Спасибо за внимание)