М, 

 ы

О  С   СВЕТА

Методы обеспечения информационной безопасности

Обеспечение информационной безопасности – это деятельность, направленная на достижение состояния защищенности (целостности, конфиденциальности и доступности) информационной среды, а также на прогнозирование, предотвращение и смягчение последствий любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре.

Укажите человека , занимающегося информационной безопасностью

1

2

3

4

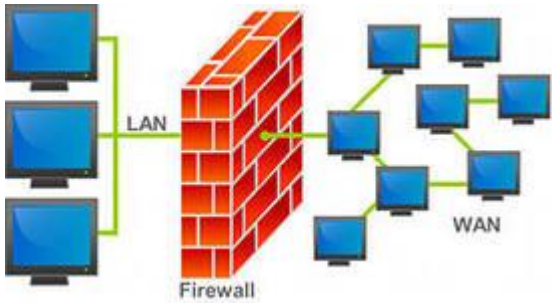
5

6

Классификация методов защиты

Технические средства защиты

- Системы шифрования
- Аутентификации
- Авторизации
- Аудита
- Антивирусной защиты
- Межсетевые экраны



Укажите методы ИБ, представленные ниже

- Сфера законодательства
- Морально-этические нормы
- Просветительная работа
- Административные меры.

Физические средства защиты

- Замки
- Камеры наблюдения
- Охранные системы

Данные, записанные на съемный носитель, помещенный в сейф в хорошо охраняемом помещении, очевидно, более защищены, чем данные, хранящиеся на диске работающего в сети компьютера, защищенного самым совершенным сетевым экраном.

- **Резервное копирование** — это набор автоматизированных процедур создания и поддержания копий данных, которые могут быть использованы для восстановления исходных данных в случае их потери или искажения.

Резервные копии записывают на сменные носители большой емкости, например магнитные ленты, которые для повышения отказоустойчивости размещают в местах, территориально разнесенных с местонахождением исходных данных.

Какие устройства наиболее подходят для резервного копирования данных?

Для эффективного поддержания информационной безопасности необходим **системный подход.** Это означает, что различные средства защиты (технические, юридические, административные, физические и т. д.) должны применяться совместно и под централизованным управлением.

Политика безопасности

Организация служб безопасности сети требует тщательной проработки **политики информационной безопасности**.

Базовые принципы ПБ

- Предоставление каждому сотруднику предприятия того **минимального уровня привилегий** на доступ к данным, который необходим ему для выполнения его должностных обязанностей.
- Использование **многоуровневого подхода** к обеспечению безопасности. Система защиты с многократным резервированием средств безопасности увеличивает вероятность сохранности данных.

Базовые принципы ПБ

- Принцип **единого контрольно-пропускного пункта** заключается в том, что весь входящий во внутреннюю сеть и выходящий во внешнюю сеть трафик проходит через единственный узел сети, например через сетевой экран. Только это позволяет в достаточной степени кон-тролировать трафик.

Базовые принципы ПБ

- Используя многоуровневую систему защиты, важно обеспечивать **баланс надежности защиты всех уровней.**

Базовые принципы ПБ

- Использование только таких средств, которые при отказе переходят в состояние **максимальной защиты.**

- Принцип **баланса возможного ущерба от реализации угрозы и затрат на ее предотвращение.** Ни одна система безопасности не гарантирует защиту данных на уровне 100 %, поскольку является результатом компромисса между возможными рисками и возможными затратами.