Петербургский государственный университет
путей сообщения Императора Александра I

Кафедра «Электрическая связь»

Современные системы и методы обеспечения информационной безопасности телекоммуникационных сетей Цифровой железной дороги

Лектор:
д.в.н., проф. Привалов А.А.

Санкт-Петербург
2019

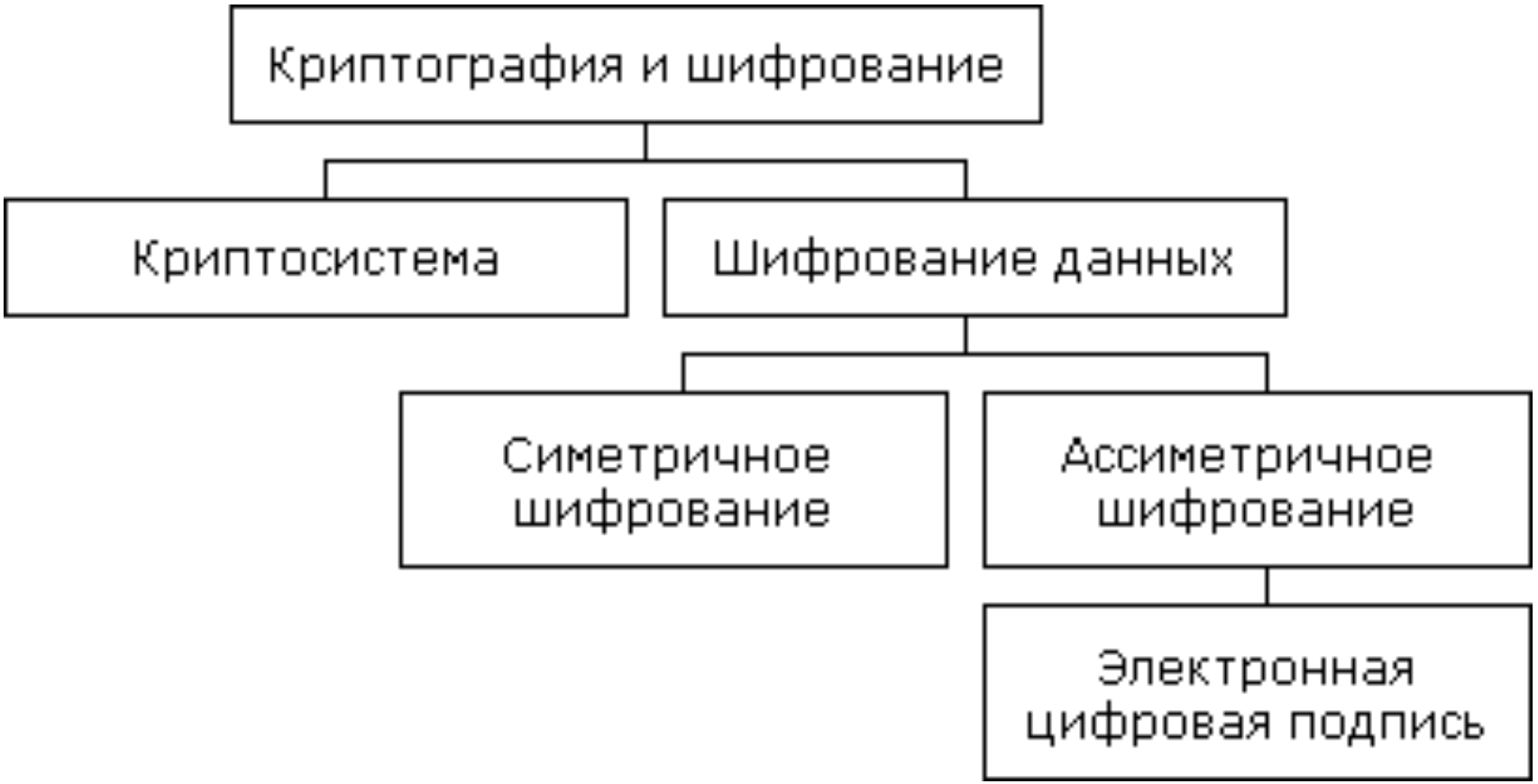
Рассматриваемые вопросы:

1. Механизмы идентификации и аутентификации пользователей.
2. Криптография и шифрование.
3. Методы разграничение доступа.
4. Регистрация и аудит ИБ.
5. Межсетевое экранирование.
6. Технология виртуальных частных сетей (VPN).

Механизмы идентификации и аутентификации пользователей

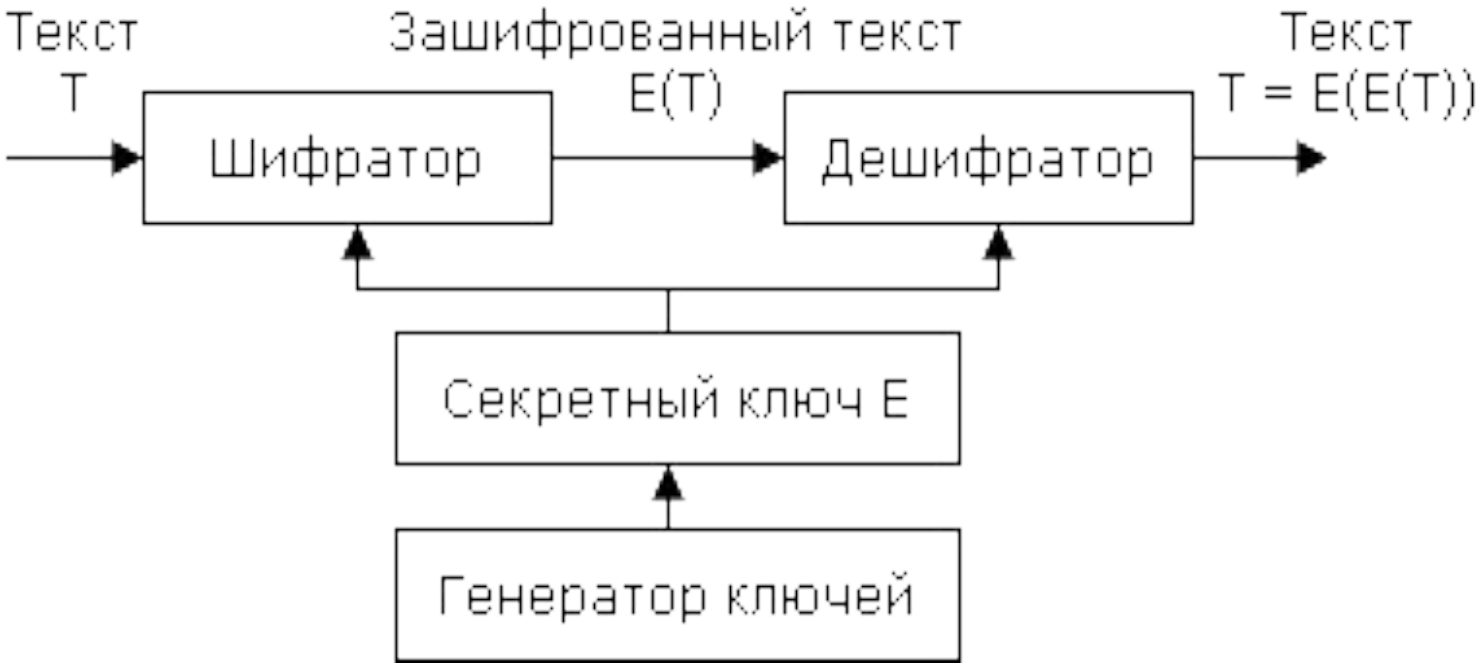
- Идентификация и аутентификации применяются для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы).
- Общий алгоритм работы таких систем заключается в том, чтобы получить от субъекта (например, пользователя) информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить (или не предоставить) этому пользователю возможность работы с системой.
- **Идентификация** – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.
- **Аутентификация** (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.
- В качестве идентификаторов в системах аутентификации обычно используют набор символов (пароль, секретный ключ, персональный идентификатор и т. п.), который пользователь запоминает или для их запоминания использует специальные средства хранения (электронные ключи). В системах идентификации такими идентификаторами являются физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза и т. п.) или особенности поведения (особенности работы на клавиатуре и т. п.).
- В последнее время получили распространение комбинированные методы идентификации и аутентификации, требующие, помимо знания пароля, наличие карточки (token) – специального устройства, подтверждающего подлинность субъекта.
- Если в процессе аутентификации подлинность субъекта установлена, то система защиты информации должна определить его полномочия (совокупность прав). Это необходимо для последующего контроля и разграничения доступа к ресурсам.
- В целом аутентификация по уровню информационной безопасности делится на три категории: статическая аутентификация, устойчивая аутентификация и постоянная аутентификация.
- Постоянная аутентификация является наиболее надежной, поскольку обеспечивает идентификацию каждого блока передаваемых данных, что предохраняет их от несанкционированной модификации или вставки.

Криптография и шифрование

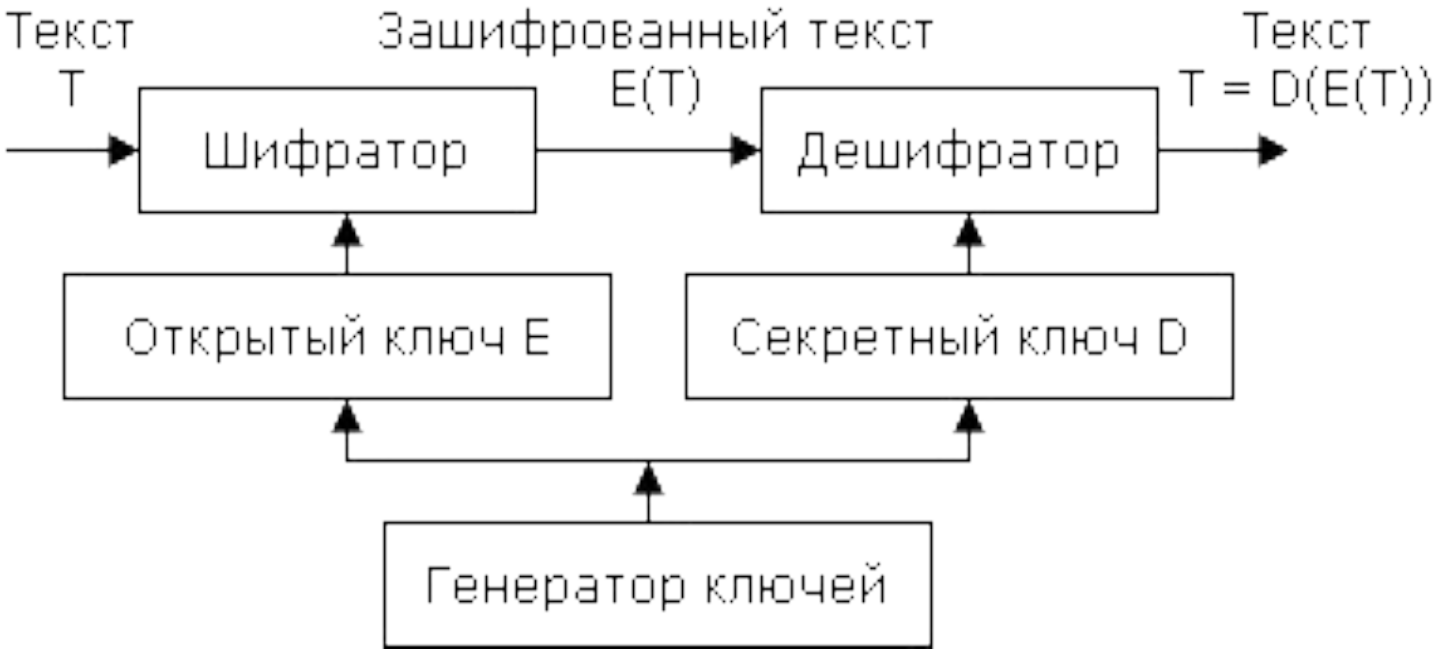


Криптография и шифрование

Криптография и шифрование

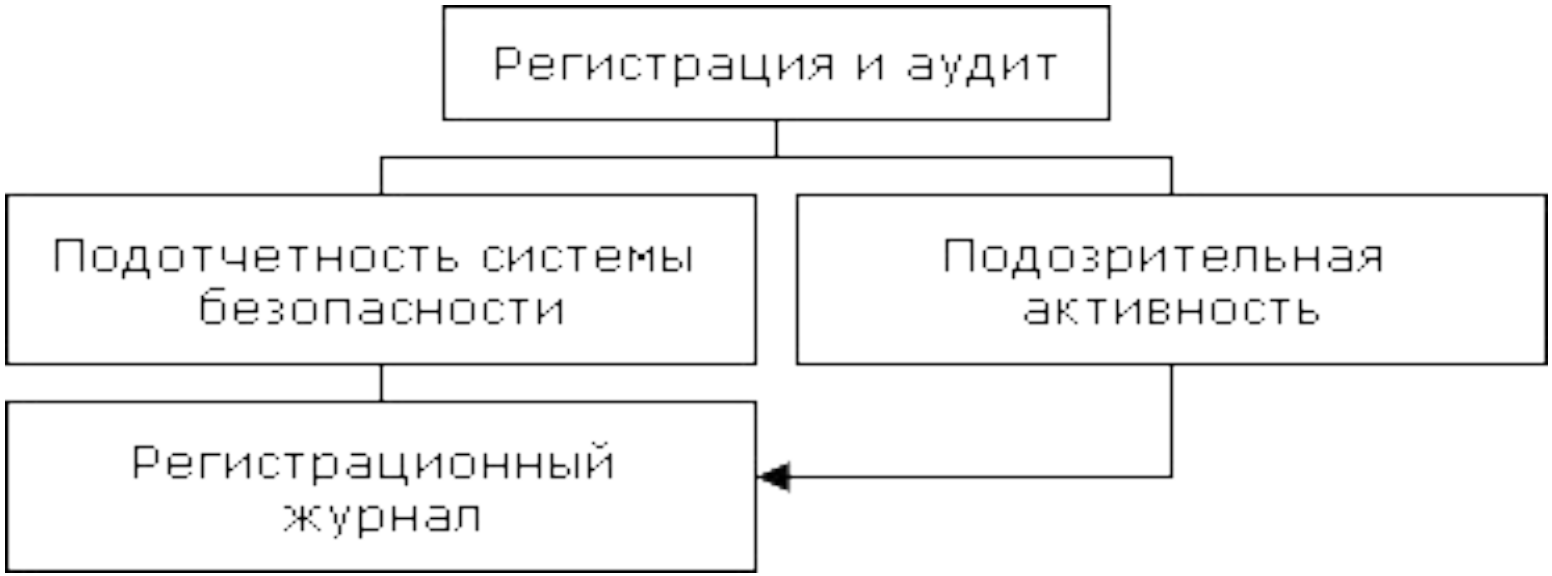


Криптография и шифрование



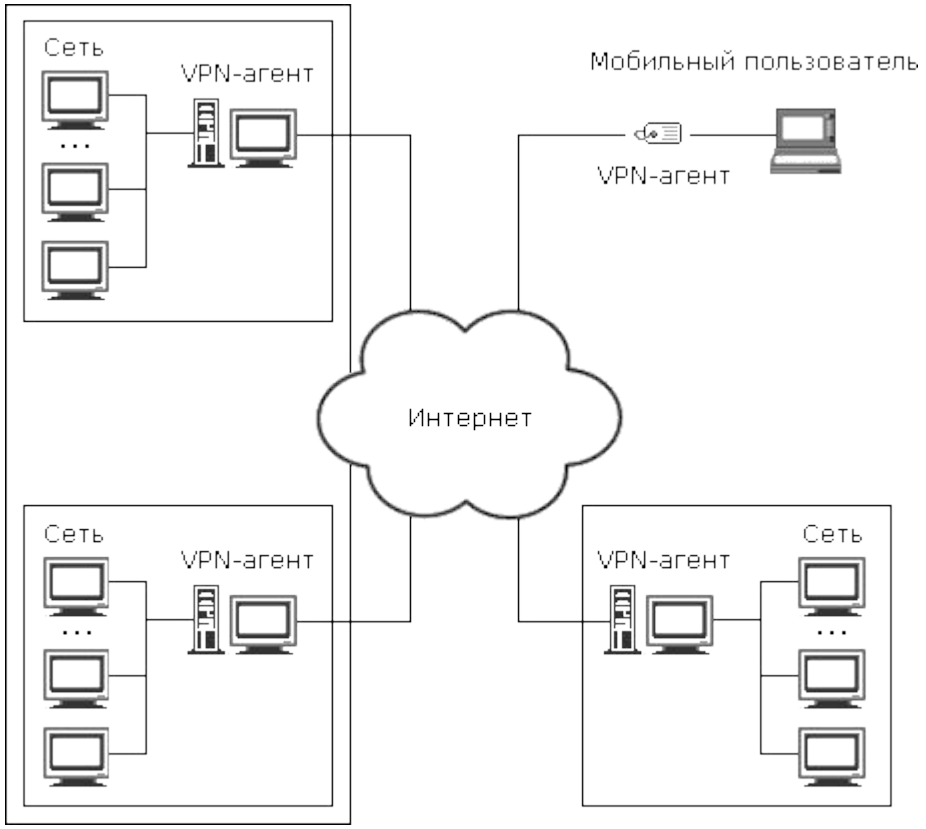
Методы разграничение доступа

Регистрация и аудит ИБ



Межсетевое экранирование

Технология виртуальных частных сетей (VPN)



Литература:

1. Спортак Марк, Паппас Френк. Компьютерные сети и сетевые технологии. – М.: ТИД "ДС", 2002.
2. Грязнов Е., Панасенко С. Безопасность локальных сетей – Электрон. журнал "Мир и безопасность" № 2, 2003. – Режим доступа к журн.: www.daily.sec.ru..
3. Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. – М.: Издательство Молгачева С. В., 2001.
4. Климов С.М. Методы и модели противодействия компьютерным атакам.- Люберцы: Каталист, 2008г., 316с.
5. В. Г. Олифер, Н. А. Олифер. Компьютерные сети. Принципы, технологии, протоколы. – СПб: Питер, 2000.

СПАСИБО ЗА ВНИМАНИЕ