BSS for Everyone.

Самые лакомые куски для хакеров в корпоративной инфраструктуре

BSS Security

Саид Эфендиев

О чем поговорим?

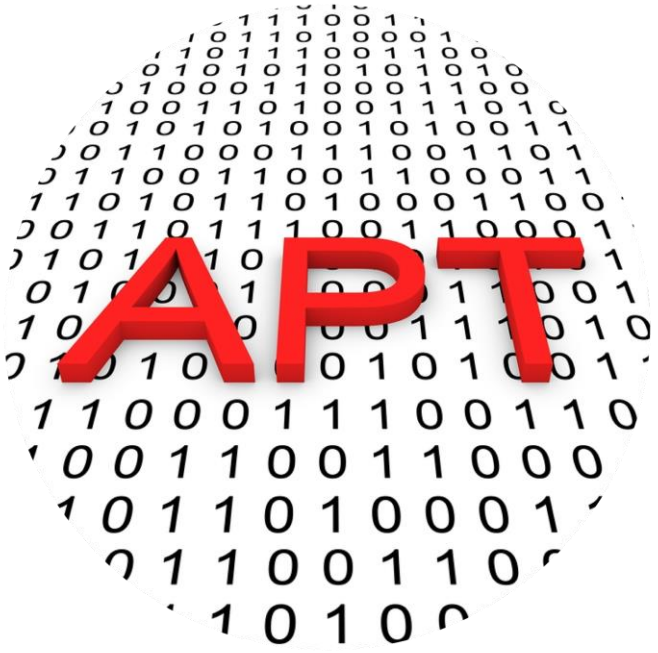
1. **Незваные гости банка.**
2. **Актуальные проблемы корпоративной инфраструктуры.**
3. **Проникновение через внешний периметр.**
4. **Взлом внутреннего периметра.**
5. **Интересы хакеров после компрометации инфраструктуры банка.**
6. **Как с этим бороться?**
7. **Немного кейсов из жизни.**

Незваные гости

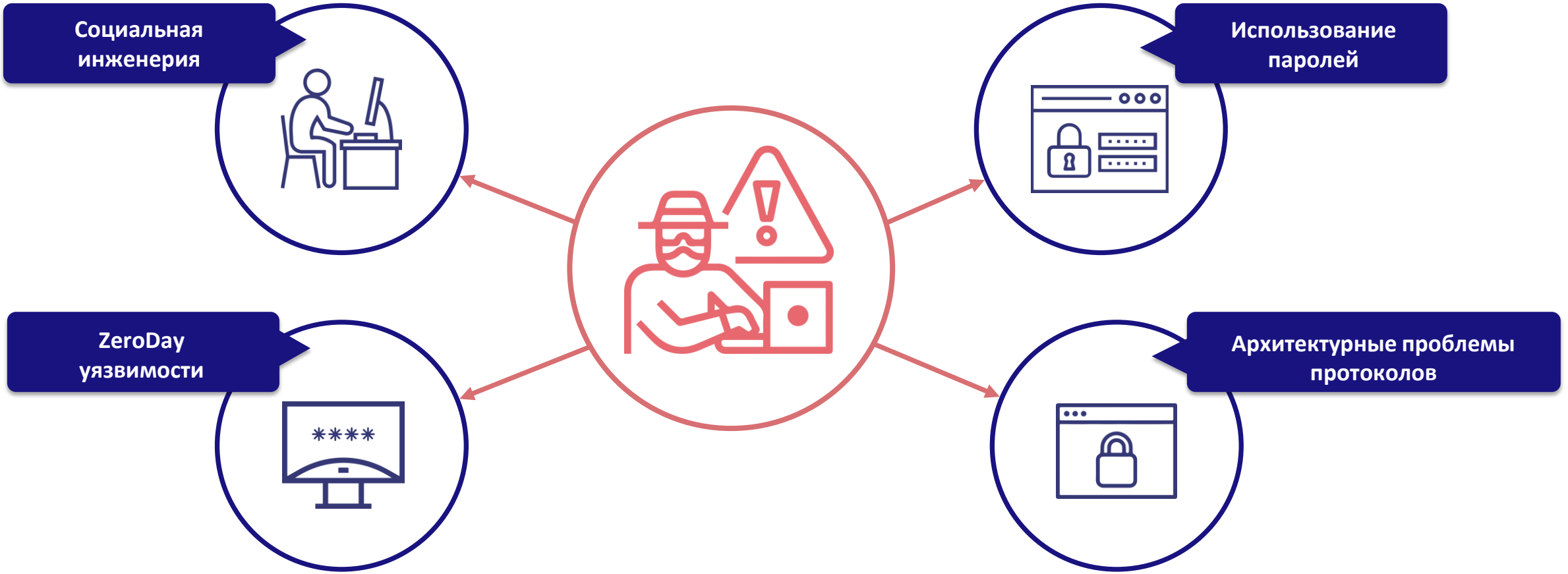
Script Kiddie

Professional

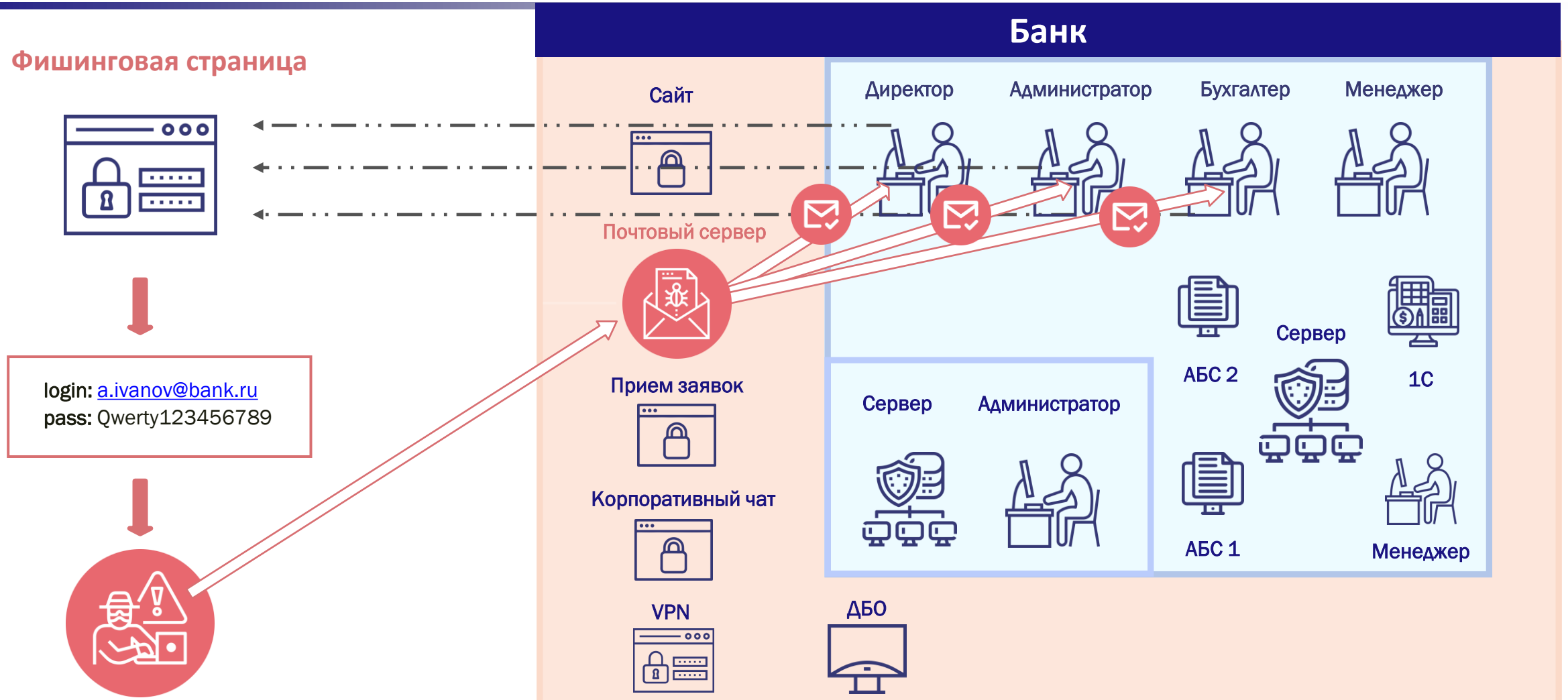
APT



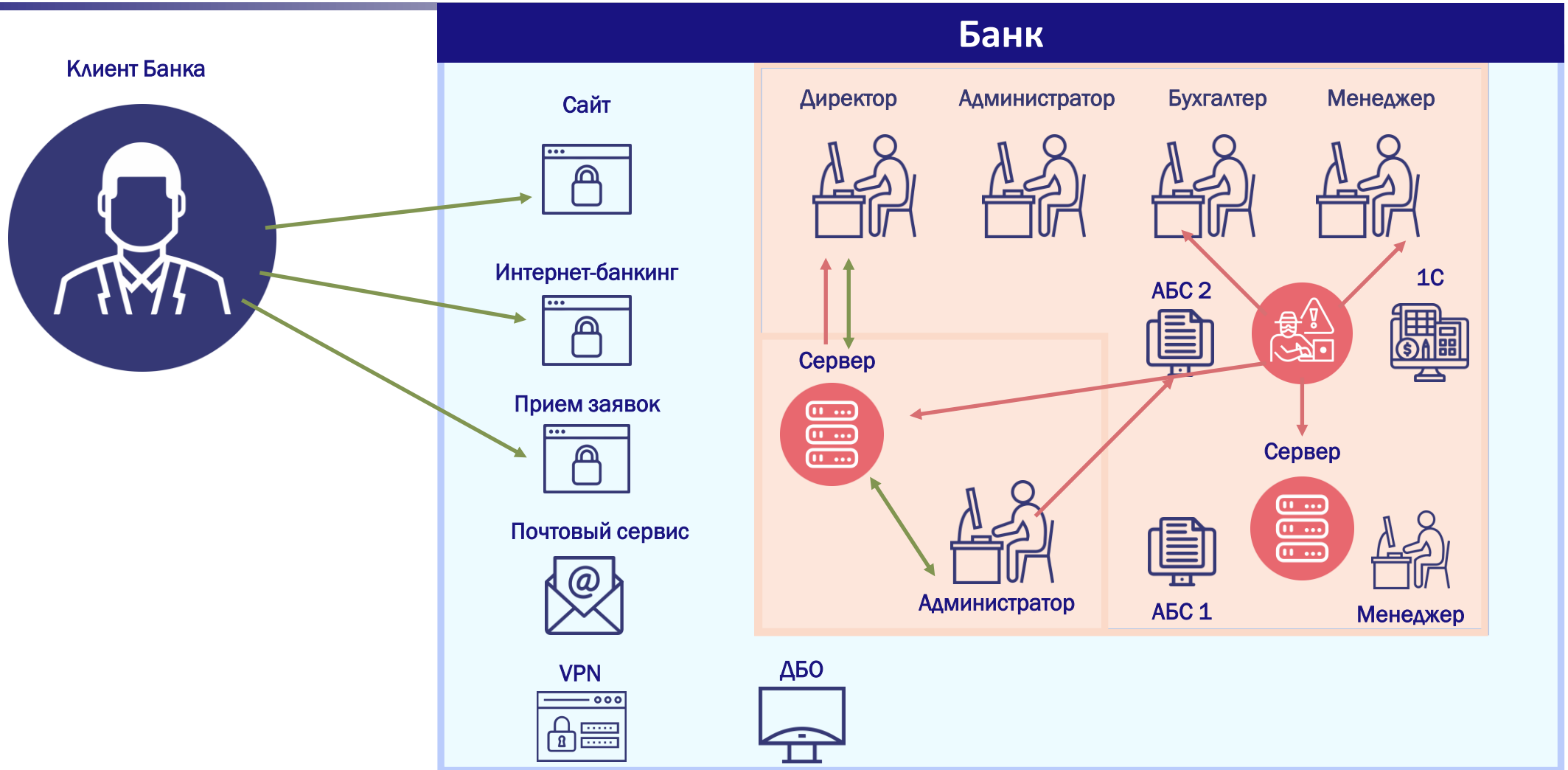
Актуальные проблемы



Внешний периметр



Внутренний периметр

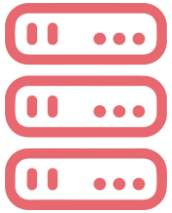


Что интересно хакерам?

Персональные данные сотрудников

Данные банковских карт

Учетные записи к сервисам



Конфиденциальные данные банка на файловом сервере

Доступ к процессингу, АБС, ДБО

Учетные записи и пароли пользователей (файл NTDS.DIT)

Рекомендации

1. **КОРРЕКТНОЕ** разделение сети на подсети:
   критическая инфраструктура,
   пользовательская подсеть,
   администраторская подсеть и др.

2. **КОРРЕКТНАЯ** реализация процесса управления доступа на уровне приложения к сервисам и системам банка.

3. Постоянное проведение тестирований и социо-тестирований.

4. Хранение паролей к системе только в защищенных хранилищах.

5. Выполнение всех рекомендаций безопасности поставщика ПО (Windows, Linux).

Кейсы из жизни

Кейс 1.

Социо-сценарий Covid + архитектурные проблемы Windows.

Кейс 2.

Приложение собственной разработки + слабые пароли.

BSS for Everyone.

Спасибо за внимание!

security@bssys.com

WWW.BSSYS.COM