AGRG

WE'RE TRANSFORMING SECURITY

SAY FUTURE

MOSCOW

"Применение СКУД для защиты информации в серверных шкафах. Соответствие требованиям стандарта PCI DSS (опыт и практика). cod.agrg.ru"

#УТЕЧКИДАННЫХ

«Сбербанк» подозревает одного из сотрудников в утечке данных 5000 клиентов. В «Сбербанке» предполагают, что кто-то из сотрудников разобрал компьютер, на котором хранились данные клиентов, и забрал жёсткий диск («Ведомости»);

«Коммерсантъ»: данные почти 9 млн клиентов «Билайна» оказались в открытом доступе;

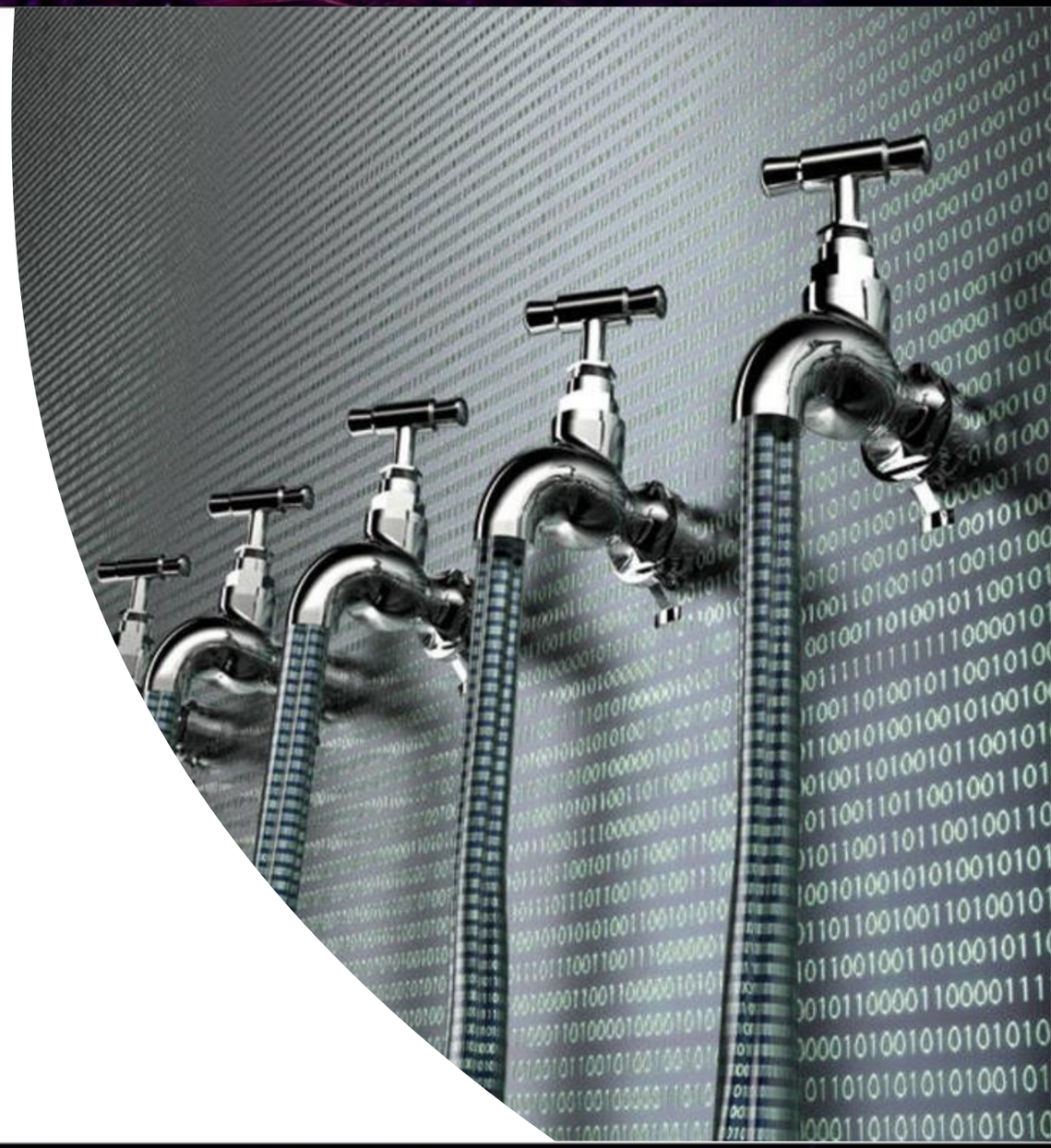
Британская исследовательская компания нашла в открытом доступе налоговые данные 20 млн россиян («Коммерсантъ»)

РЖД начала проверку после утечки персональных данных 703 тысяч человек — предположительно, сотрудников компании

Данные пассажиров надёжно защищены, заверили в РЖД.

Данные клиентов ОТП-банка, Альфа-банка и ХКФ-банка оказались в открытом доступе. Утечка суммарно затрагивает интересы примерно 900 тыс. россиян (DeviceLock)

Взлом банковского холдинга Capital One привел к утечке данных более 106 млн человек (HABR.COM)



ЗАЩИТА ДАННЫХ. РОСТ СПРОСА НА РЕШЕНИЯ

CASTLE ЦОД

Комплекс мониторинга и контроля доступа ИТ-инфраструктуры

PCI DSS – ТРЕБОВАНИЯ К ЗАЩИТЕ ФИНАНСОВОЙ ИНФОРМАЦИИ

PCI DSS (Payment Card Industry **Data Security Standard**) — **стандарт безопасности данных индустрии платёжных карт**, разработанный Советом по стандартам безопасности индустрии платежных карт. Стандарт представляет собой совокупность 12 детализированных требований по обеспечению безопасности данных о держателях платёжных карт, которые передаются, хранятся и обрабатываются в информационных инфраструктурах организаций.

PCI DSS И КОНТРОЛЬ ДОСТУПА

Построить и поддерживать защищенные сети и системы	1.	Установить и поддерживать конфигурацию межсетевых экранов для защиты ДДК.
	2.	Не использовать пароли к системам и другие параметры безопасности по умолчанию, заданные производителем.
Защищать ДДК	3.	Защищать хранимые ДДК
	4.	Шифровать ДДК при передаче через сети общего пользования.
Поддерживать программу управления уязвимостями.	5.	Защищать все системы от вредоносного ПО и регулярно обновлять антивирусные ПО или программы
	6.	Разрабатывать и поддерживать безопасные системы и приложения
Внедрять строгие меры контроля доступа	7.	Ограничивать доступ к ДДК в соответствии со служебной необходимостью.
	8.	Идентифицировать и аутентифицировать доступ к системным компонентам
	9.	Ограничивать физический доступ к ДДК
Осуществлять регулярный мониторинг и тестирование сетей	10.	Отслеживать и вести мониторинг всего доступа к сетевым ресурсам и ДДК
	11.	Регулярно тестировать системы и процессы безопасности
Поддерживать политику информационной безопасности	12.	Поддерживать политику информационной безопасности для всех работников.

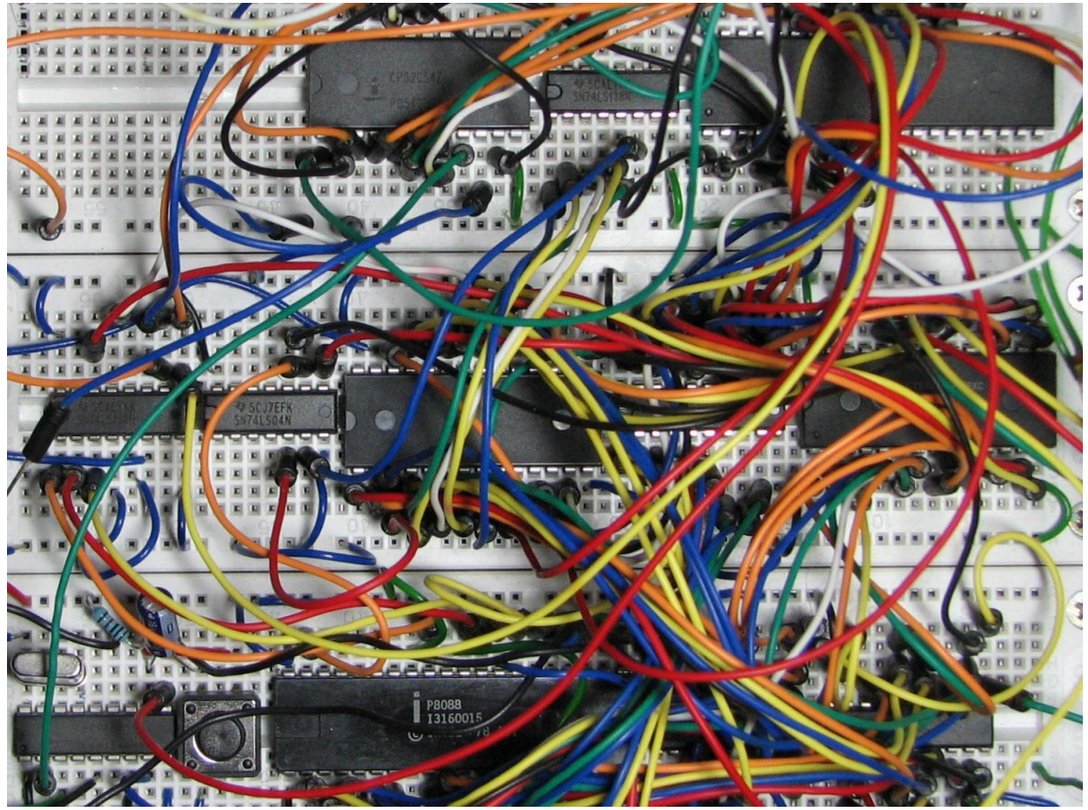
**ДДК – данные держателей карт*

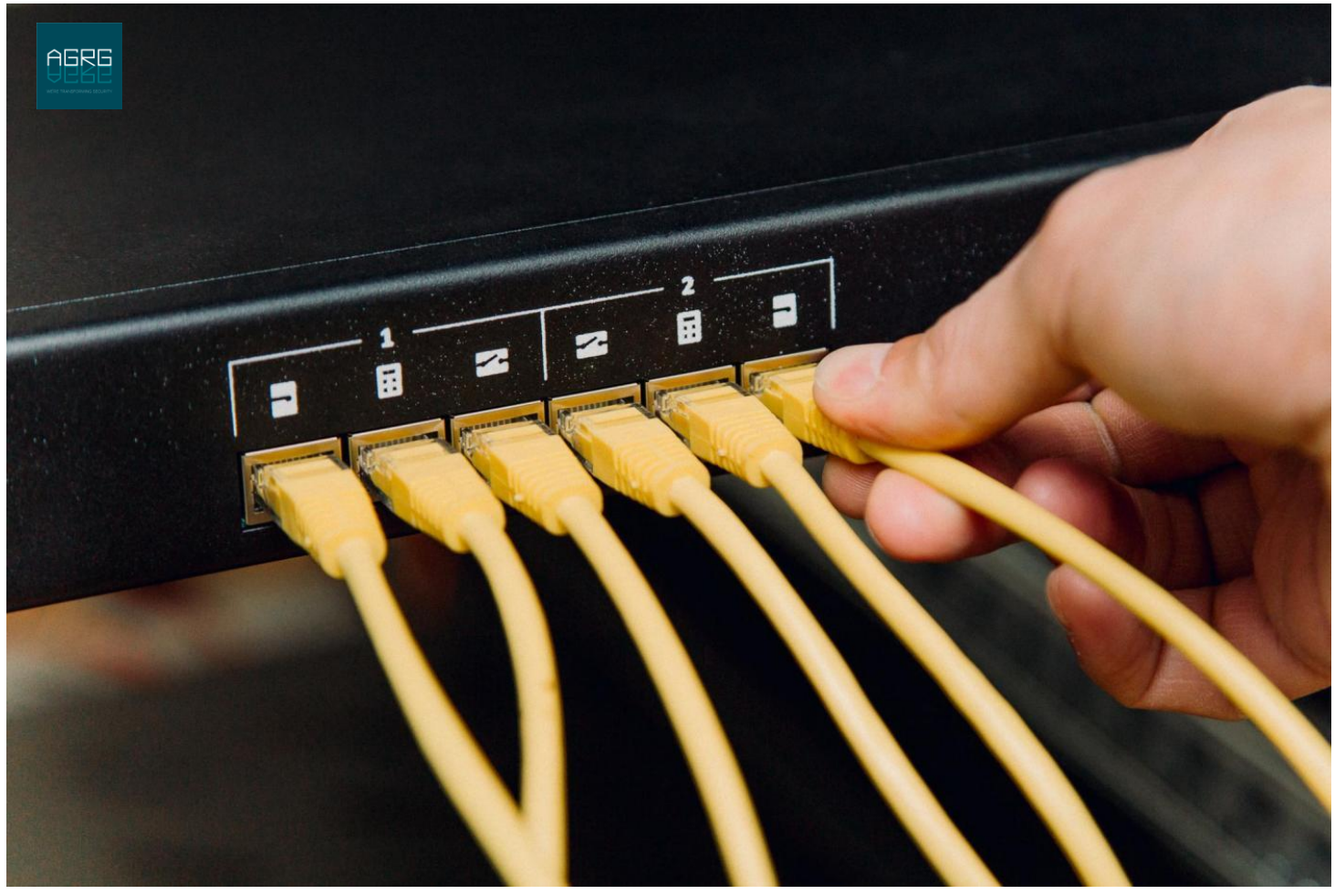
PCI DSS В НЕСЕРТИФИЦИРОВАННОМ ЦОД

1. ЦОД - незащищенная территория со свободным доступом.
2. Шкаф должен быть защищен. На нем должно быть:
- все стенки и дверцы;
- камеры видеонаблюдения;
- специализированные замки;
- датчики открытия каждой двери.
3. Создать и внедрить процедуру управления доступом;
4. Внутри шкафа установить и настроить СКУД и видеорегистратор;
5. Автоматически уведомлять ответственных сотрудников о фактах открытия шкафа;
6. Регулярный анализ данных систем видеонаблюдения и СКУД;
7. Все кабели и разъемы располагаются только внутри шкафа;

Рекомендации QSA-аудитора (Qualified Security Assessor)

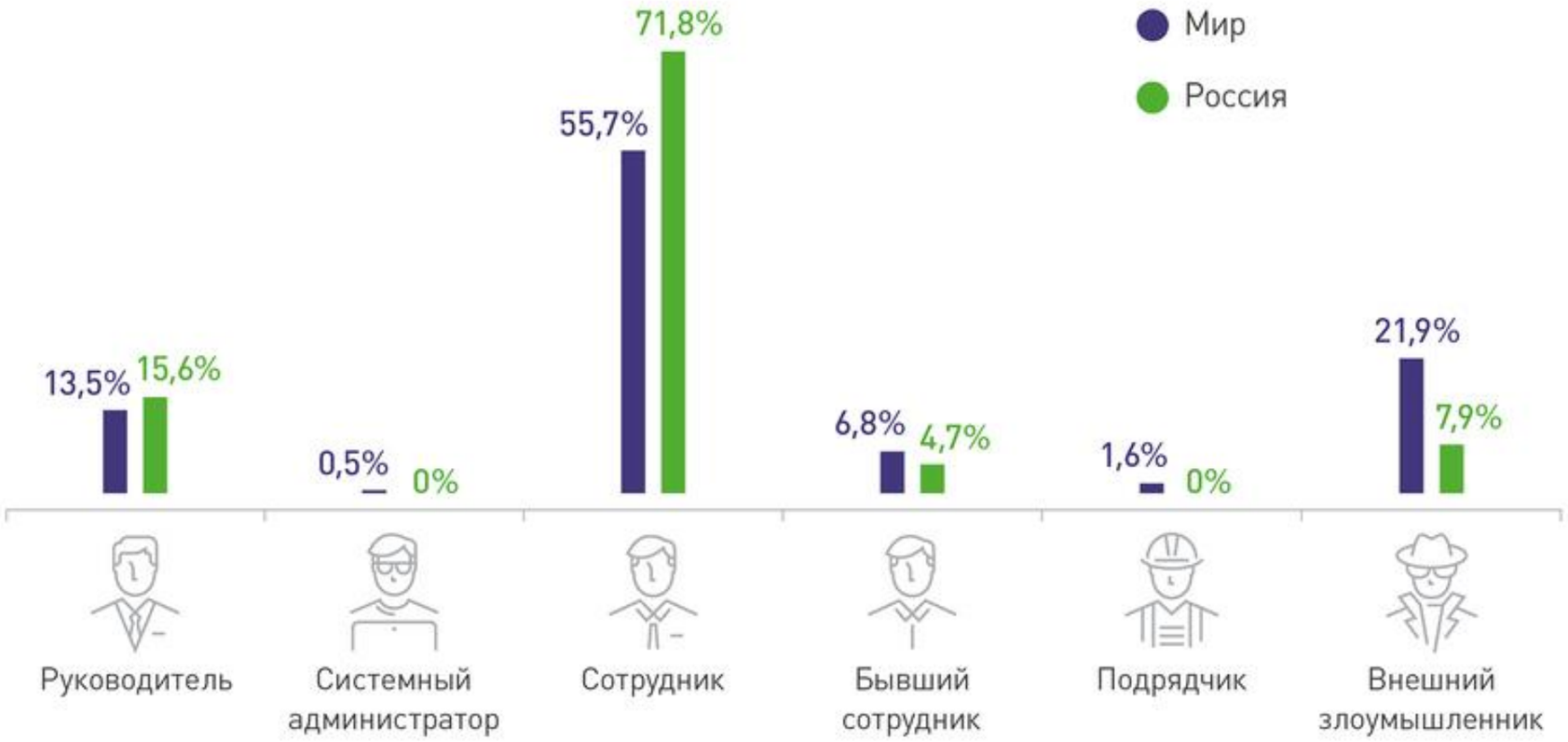
КОНТРОЛЬ ДОСТУПА В ЦОД. КАК ДЕЛАЮТ И КАК НАДО.

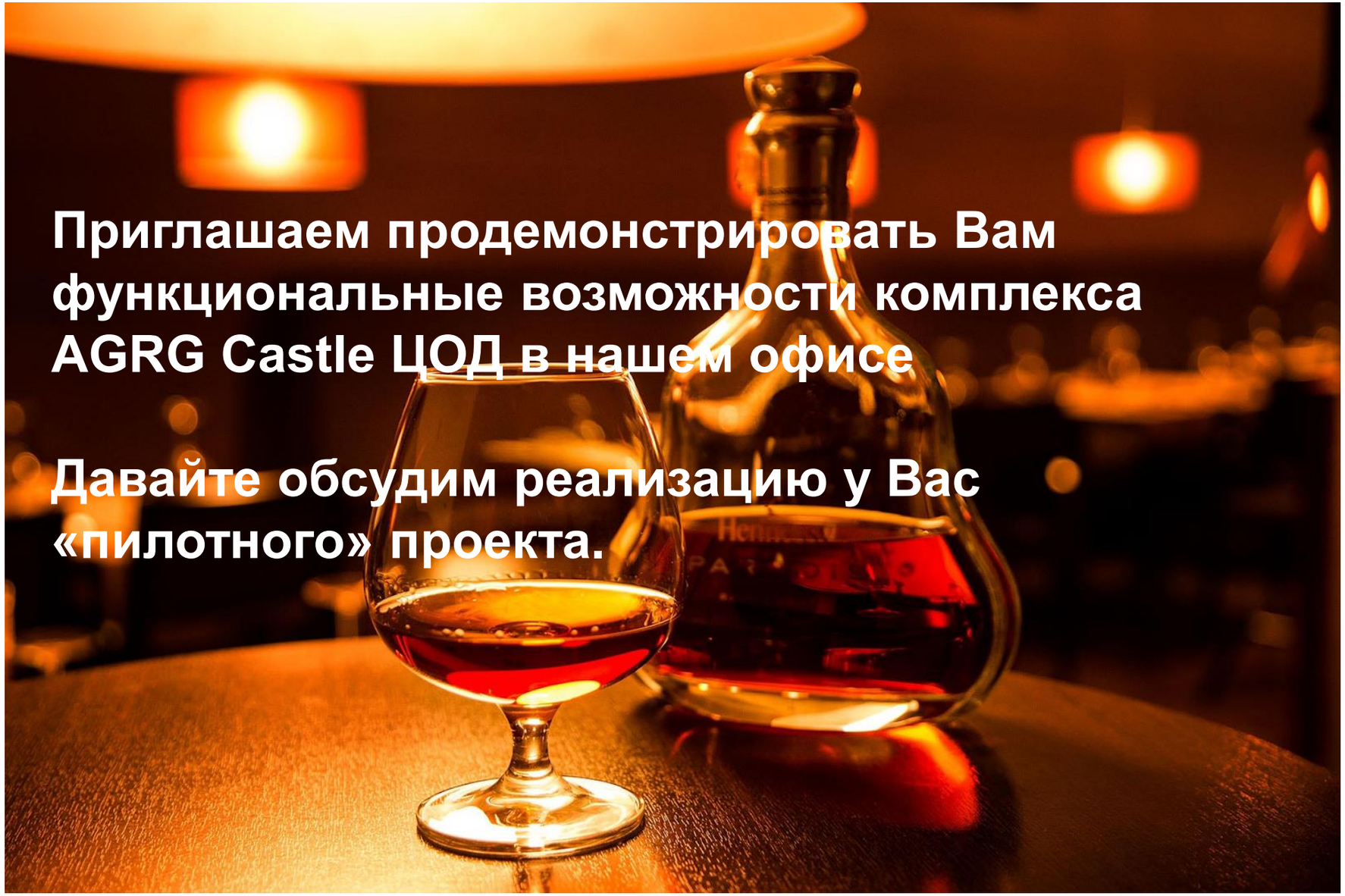




ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ. ЗАКОНОПРОЕКТ № 729516-7

Распределение мошеннических инидентов с данными по виновникам, мир — Россия, 2018





Приглашаем продемонстрировать Вам функциональные возможности комплекса AGRG Castle ЦОД в нашем офисе

Давайте обсудим реализацию у Вас «пилотного» проекта.

WE'RE TRANSFORMING SECURITY

Связаться
Телефон: +7 (495) 988-9116
E-mail: info@agrg.ru
Отдел продаж: sale@agrg.ru

https://cod.agrg.ru/