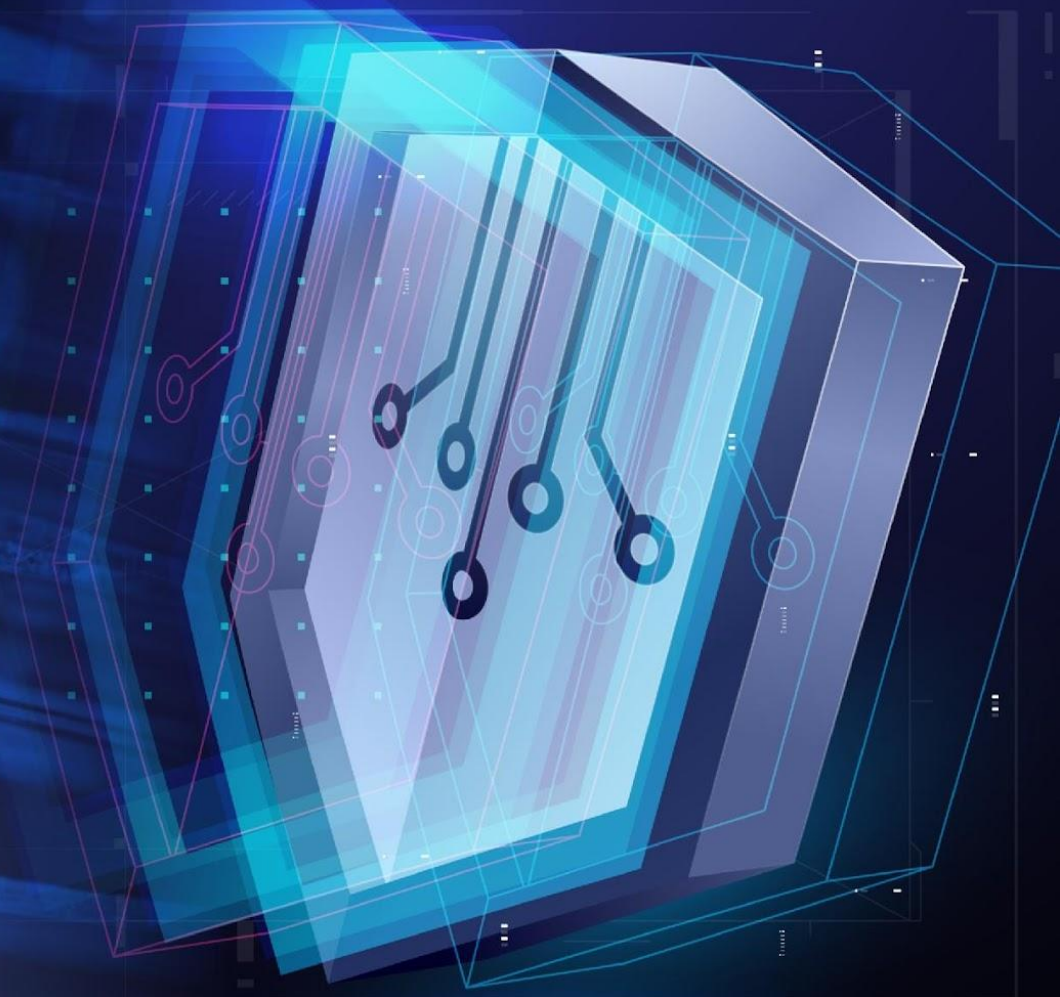
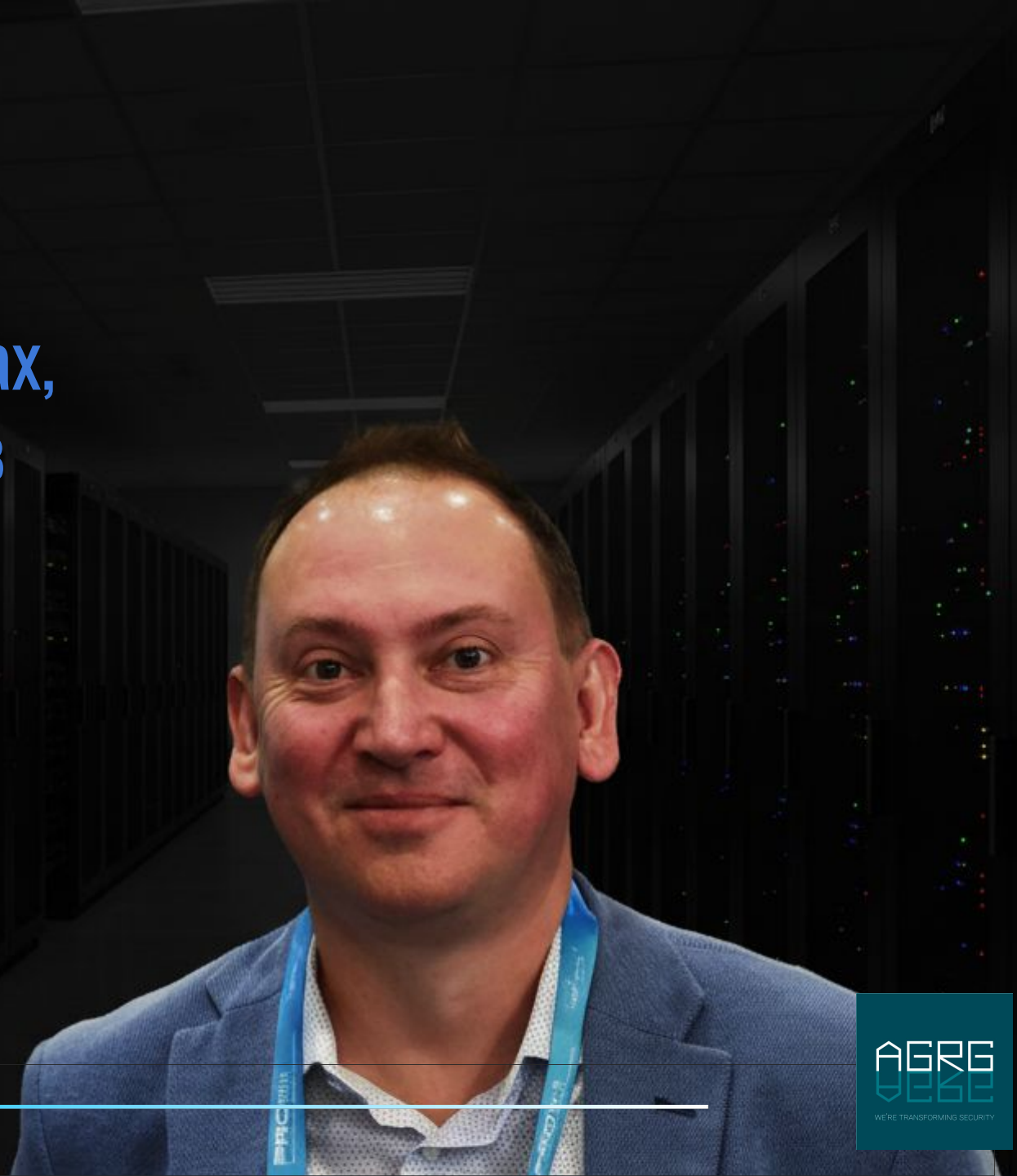
ОСЕННИЙ ФОРУМ`25



Меня зовут Александр Чижов.

Сегодня я расскажу о двух вещах, которые меняют правила игры в 2026 году:

Что защита ИБ начинается не с софта, защита ИБ начинается с замка на телеком-шкафе.



— и о дизайнерских считывателях, от которых сложно отвести взгляд

Взломы растут, атаки усложняются, а штрафы становятся разрушительными

— пришло время пересмотреть физическую безопасность критической инфраструктуры.

AGRG
WE'RE TRANSFORMING SECURITY

Защита от внешнего, внутреннего нарушителя и нанесения им ущерба активам предприятия, кражи данных из шкафов ЦОД или серверных комнат. Защита от похищения HDD с конфиденциальными данными собственника

Случайное или злонамеренное нарушение регламента обслуживания сотрудником, приведшее к краже или удалению конфиденциальных данных.

При наличии AGRG ручек вы владеете информацией о времени доступа, личности сотрудника, можете соотнести доступ определенного сотрудника и возникновение проблем.

Открытый серверный шкаф — риск кражи, удаления или подмены данных, заражения вирусами и остановки работы компании.

Рынок физической защиты данных в России еще формируется, и требования разбросаны по множеству регламентов, включая международные, при разработке мы учитывали:

ФЗ-187 «О безопасности критической информационной инфраструктуры Российской Федерации» от 01.01.2018 г.	Статья 10.
ФЗ-152 «О персональных данных» от 27.07.2006 г.	Статья 19.
Постановление Правительства РФ от 01.11.2012г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"	https://base.garant.ru/70252506/
Приказ ФСТЭК от 18.02.2013 г. №21 определяет требования к мерам по обеспечению безопасности ПД в ИСПДн	ЗНИ.4, ЗТС.2, ЗТС.3
Банк данных угроз безопасности информации ФСТЭК. УБИ.139 Угроза преодоления физической защиты.	Описание угрозы, Объект воздействия : сервер, рабочая станция, носитель информации, аппаратное обеспечение, Последствия реализации угрозы Нарушение конфиденциальности, Нарушение целостности, Нарушение доступности
ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер».	Пункты 7.2.3, 7.2.3.1, 7.2.3.2 7.2.3.3, 7.2.3.4
СН 512-78 Правительства РФ. Технические требования к зданиям и помещениям для установки средств вычислительной техники.	Пункт 3.11.
ГОСТ Р 50739 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.	Защищенность от НСД к информации при ее обработке СВТ характеризуется тем, что только надлежащим образом уполномоченные лица или процессы, инициированные ими, будут иметь доступ к чтению, записи, созданию или уничтожению информации. И Пункты 5.1, 5.1.1
PCI DSS Требование 9: ограничение физического доступа к данным держателей карт.	https://cod.agrg.ru/pci-dss
Р 78.36.018-2011 Рекомендации по охране особо важных объектов с применение интегрированных систем безопасности	Пункты 3.2 -3.12 (https://www.consultant.ru/document/cons_doc_LAW_256462/)

Модельный ряд

AGRG SH-I, SH-I (F)	AGRG SH-C,SH-C (F)	AGRG SH-D	AGRG SH-O (NEW)
Мультиформат, SL1, SL3	Два фактора, SL1, SL3	Автономная	OSDP + SL3!

Состав ручки и форматы карт

MIFARE (UID), Mifare Mini, Mifare Classic, Mifare Plus SL1/SL3, Mifare DESFire (UID и чтение из защищенной области карты);
Mifare ID (UID и чтение из защищенных секторов карты).
I-CODE (ISO15693) (UID);
EM-Marine (UID);
HID 125 кГц (UID);
Indala (Motorola) (UID);
и BLE при установке приложения на смартфон* (Android и Apple)
CheckPoint

Кейс 1: защита распределённой инфраструктуры с SH-I

Кто и когда. Каждый доступ фиксируется.

Невозможно подделать. MIFARE SL3 — защита на уровне криптографии.

Просто закрыт. Без карты шкаф не открыть.

Удалённое администрирование — блокировка/разрешение доступа с центрального сервера.

Снижение операционных рисков — исключение простоев и утечек данных.

Совместимость — интеграция с системой контроля и управления доступом **Elsys** (Полная совместимость!)

Кейс 2: защита ЦОДов с SH-C

ФЗ-187 (КИИ) и **152-ФЗ (ПДн)** обязывают защищать критическую инфраструктуру и персональные данные.

PCI DSS требует строгой аутентификации и учёта доступа для систем, где обрабатываются платёжные данные.

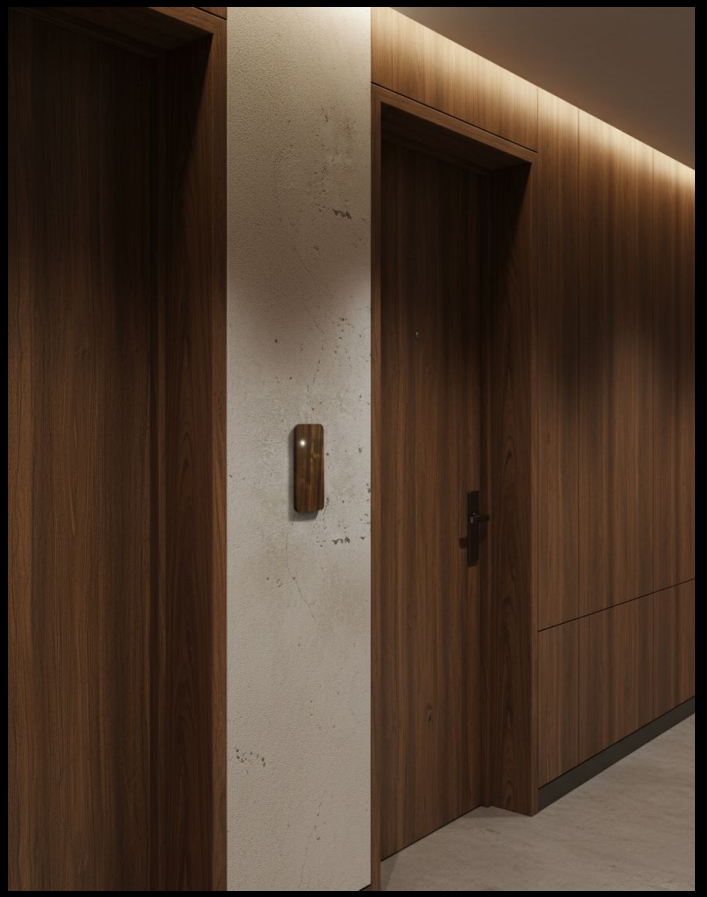
Двухфакторная идентификация. Карта + PIN → соответствие PCI DSS и требованиям регуляторов.

Соответствие нормам. Упрощение аудитов и проверок: СКУД на шкафах соответствует требованиям ФСТЭК и PCI DSS.

Наша экспертиза — больше, чем ручки. Это аксессуары. Это сотни шкафов. Это опыт.

Любые цвета.

Единый дизайн.



...и до редких пород деревьев.

Создадим устройство, которое будет идеально соответствовать вашему стилю и интерьеру:

Технологично и современно.

Просто работает. Просто красиво.

Кратко про защиту шкафов.

Дизайнерская электроника