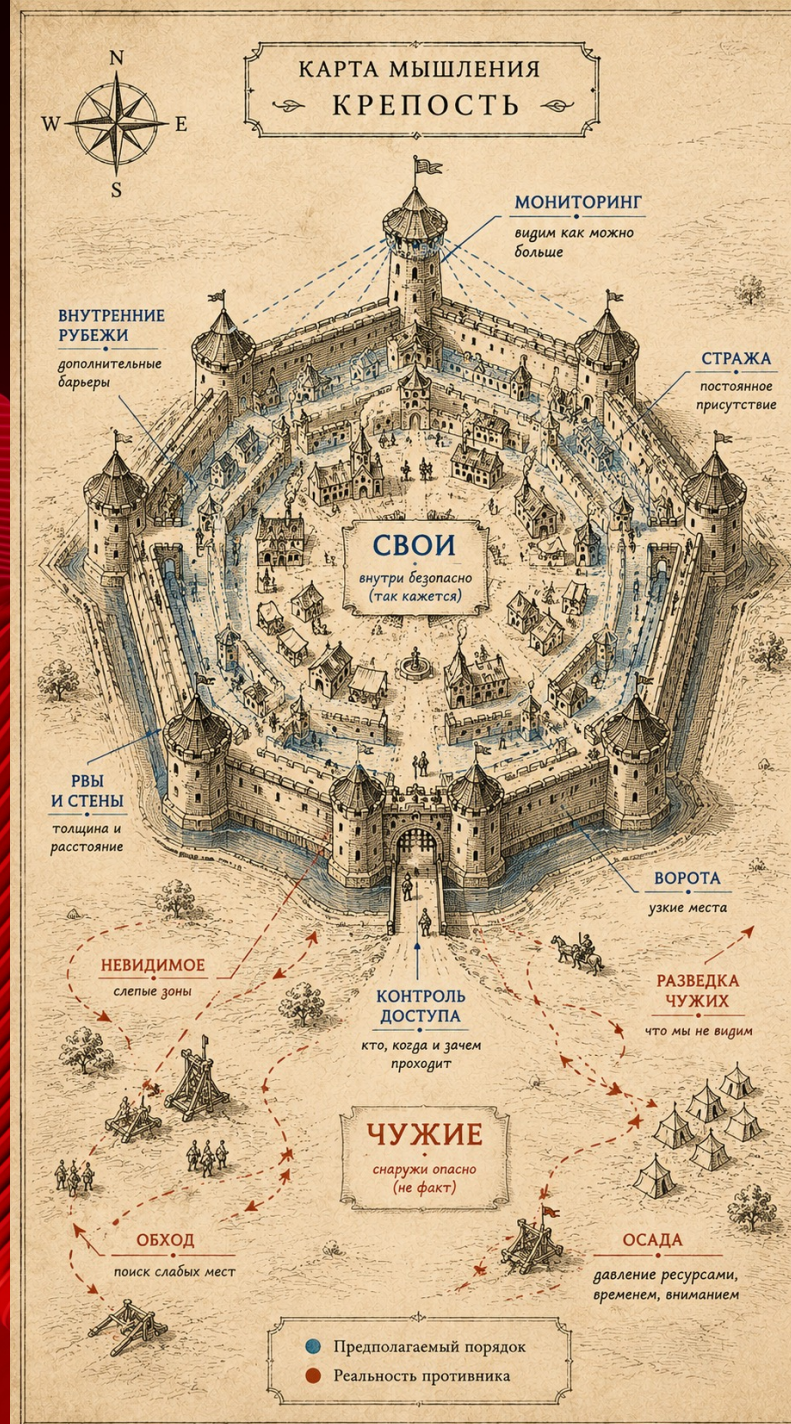


Алексей Лукацкий

Chief Evangelist Officer  
Positive Technologies

# Дрон против крепости

Почему кибербез до сих пор строит стены в эпоху асимметричных атак



# Who Am I?!

- Chief Evangelist Officer в Positive Technologies
- Автор проекта «Бизнес без опасности» и «Пост Лукацкого»
- Автор 5 книг и 30+ курсов по ИБ
- Программист, админ, аудитор, маркетолог, продавец, консультант, преподаватель, писатель, популяризатор
- 30+ лет в кибербезе



Торжественные похороны  
крепостной стены.



# Периметр умер

Но... бюджеты, архитектуры, процессы согласования, контроли доступа и отчеты аудиторов создают ощущение, что периметр не умер. Его просто забальзамировали, переименовали и превратили в «стюардессу»...

СТАРЫЕ СТЕНЫ.  
НОВЫЕ СПОСОБЫ.

ДОРОГО.  
ТЯЖЕЛО.  
ЗАМЕТНО.

# Культурный код

Когда мир становится опаснее, мы строим стену. Когда стена перестает работать, мы строим стену повыше, потолще... стену, забор, границу, ТСПУ, турникет, входную дверь...

ДЕШЕВО.  
ЛЕГКО.  
НЕЗАМЕТНО.

СТЕНЫ СОЗДАНЫ, ЧТОБЫ СТОЯТЬ.  
НО НЕ ДЛЯ ТОГО, ЧТОБЫ ВЫЖИТЬ.

# ЭВОЛЮЦИЯ ИДЕИ ПЕРИМЕТРА: ОТ ПРИРОДЫ К ЦИВИЛИЗАЦИИ

①  
ТЕРМИТНИК  
защита через  
структуру



угроза  
снаружи

②  
БИЗОНЫ  
круг ради  
защиты слабых



угроза  
снаружи

③  
ВЕЛИКАЯ  
КИТАЙСКАЯ  
СТЕНА  
периметр  
на века



угроза  
снаружи

④  
КИБИТКИ  
НА ДИКОМ  
ЗАПАДЕ  
круг в пути –  
жизнь внутри



угроза  
снаружи

⑤  
ДРЕВНЕРУССКИЕ  
ДЕТИНЦЫ  
стена, ров,  
ворота



угроза  
снаружи

ИДЕЯ ОДНА:  
СОЗДАТЬ ГРАНИЦУ, ЧТОБЫ СОХРАНИТЬ СВОЁ.

→ УГРОЗА

→ ПЕРИМЕТР / ЗАЩИТА



# Мир меняется, идея периметра не умирает. Просто стена перестает быть центром стратегии!

АТАКА НА ДОВЕРИЕ

ПРИКАЗ.  
ПРОПУСТИТЬ.

ПРОВЕРЕНО

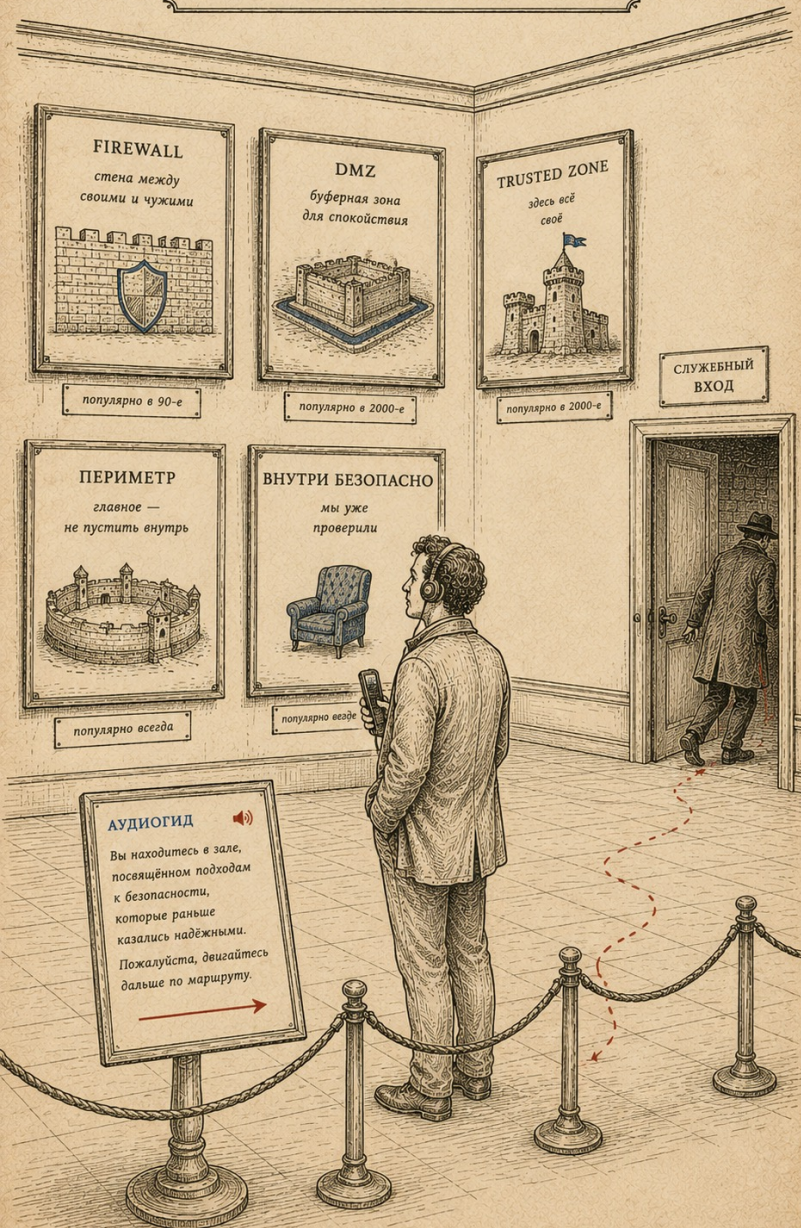
...приказываю  
открыть ворота  
и обеспечить  
беспрепятственный  
проход...СЛЕД ПОДМЕНЫ  
НЕ ВИДЕН ПРИ ДОВЕРИИ,  
ВИДЕН ПРИ ПРОВЕРКЕ.АТАКА  
подготовлена  
незаметноДОВЕРИЕ  
подтверждено  
печатьюДОСТУП  
получен  
без проверкиПЕЧАТЬ НАСТОЯЩАЯ.  
ПРИКАЗ — ЛОЖНЫЙ.

# Очень понятная идея

- Есть «МЫ»
- Есть «ОНИ»
- Есть граница
- Есть ворота
- Есть стража
- Есть иллюзия контроля

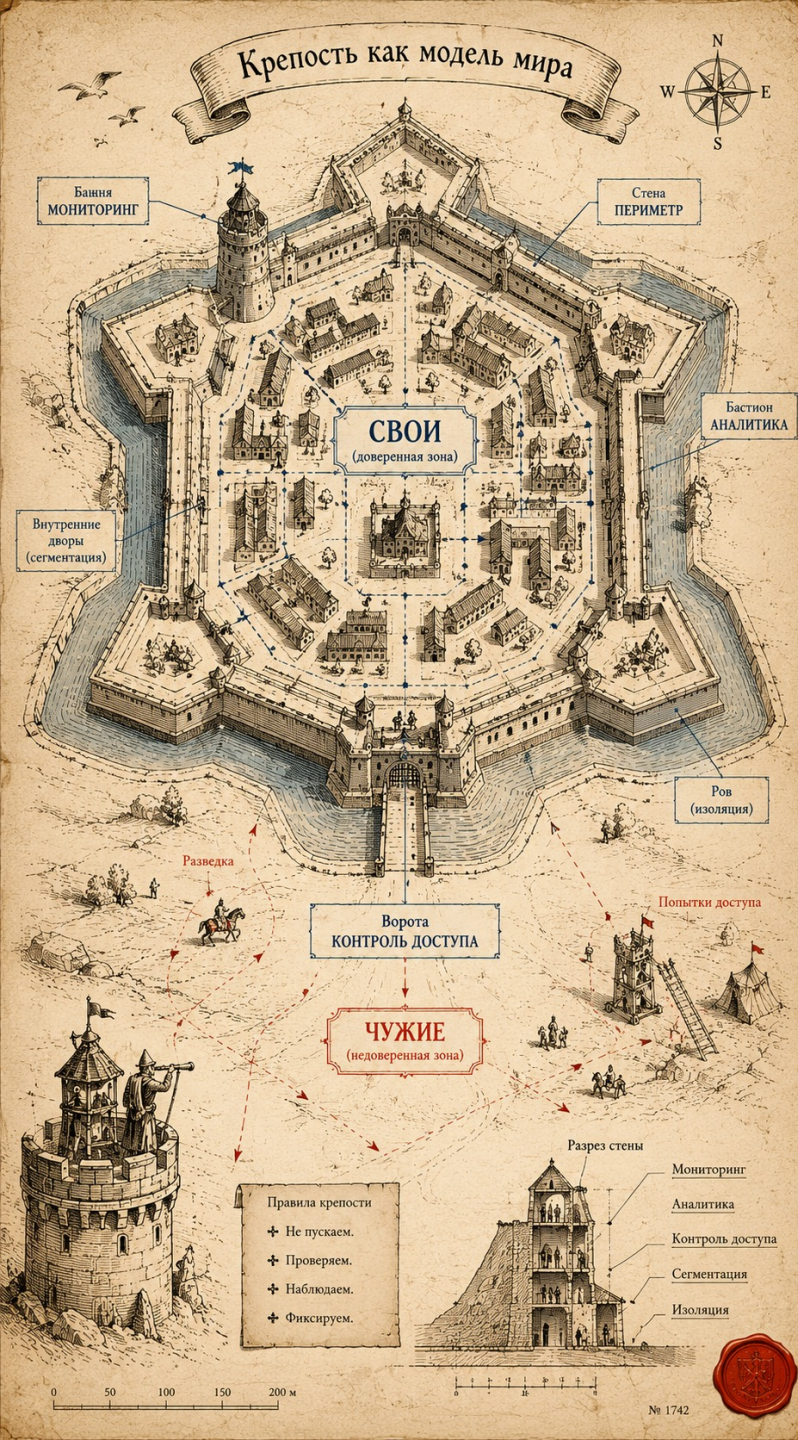
## МУЗЕЙ УСТАРЕВШИХ МЕТАФОР

экспозиция постоянная



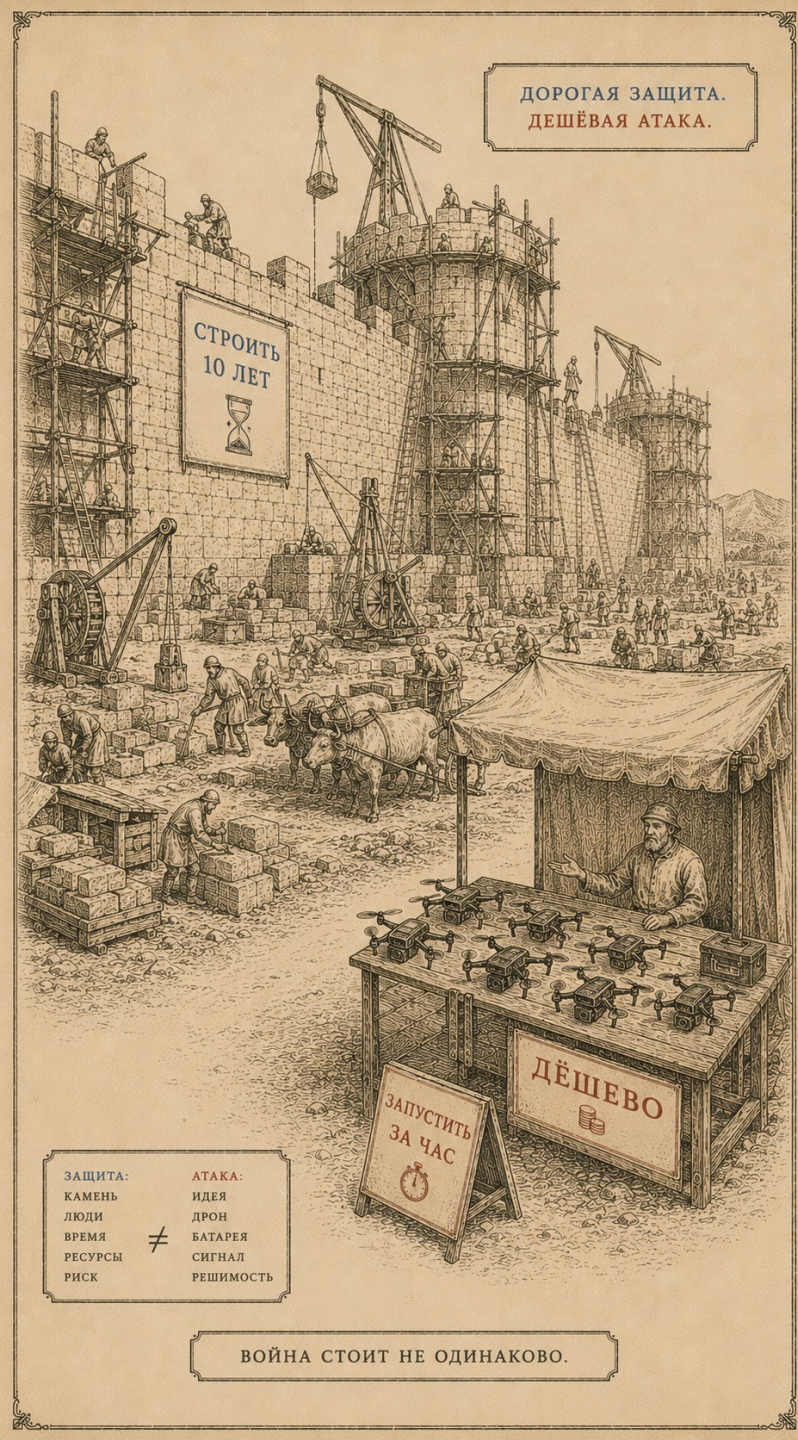
# Мир меняется, а метафора безопасности остаётся старой

«Панцирь», «Застава», «Барьер»,  
«Граница», «Кольчуга», «Бастион»,  
«Рубикон», \*Gate, \*Edge, \*Wall,  
«Стена», Gateway, «Рубеж»,  
«Цитадель»...



# Крепость – это не технология. Это способ думать!

ДОРОГАЯ ЗАЩИТА.  
ДЕШЁВАЯ АТАКА.



ЗАЩИТА:	АТАКА:
КАМЕНЬ	ИДЕЯ
ЛЮДИ	ДРОН
ВРЕМЯ	БАТАРЕЯ
РЕСУРСЫ	СИГНАЛ
РИСК	РЕШИМОСТЬ

≠

ВОЙНА СТОИТ НЕ ОДИНАКОВО.

Пушки не победили  
стену, они изменили  
ее экономику

# Крепости не исчезли — они адаптировались

- Стали ниже
- Толще
- Сложнее
- Появились бастионы
- Изменилась геометрия
- Важнее стали углы, поля обстрела, глубина, логистика

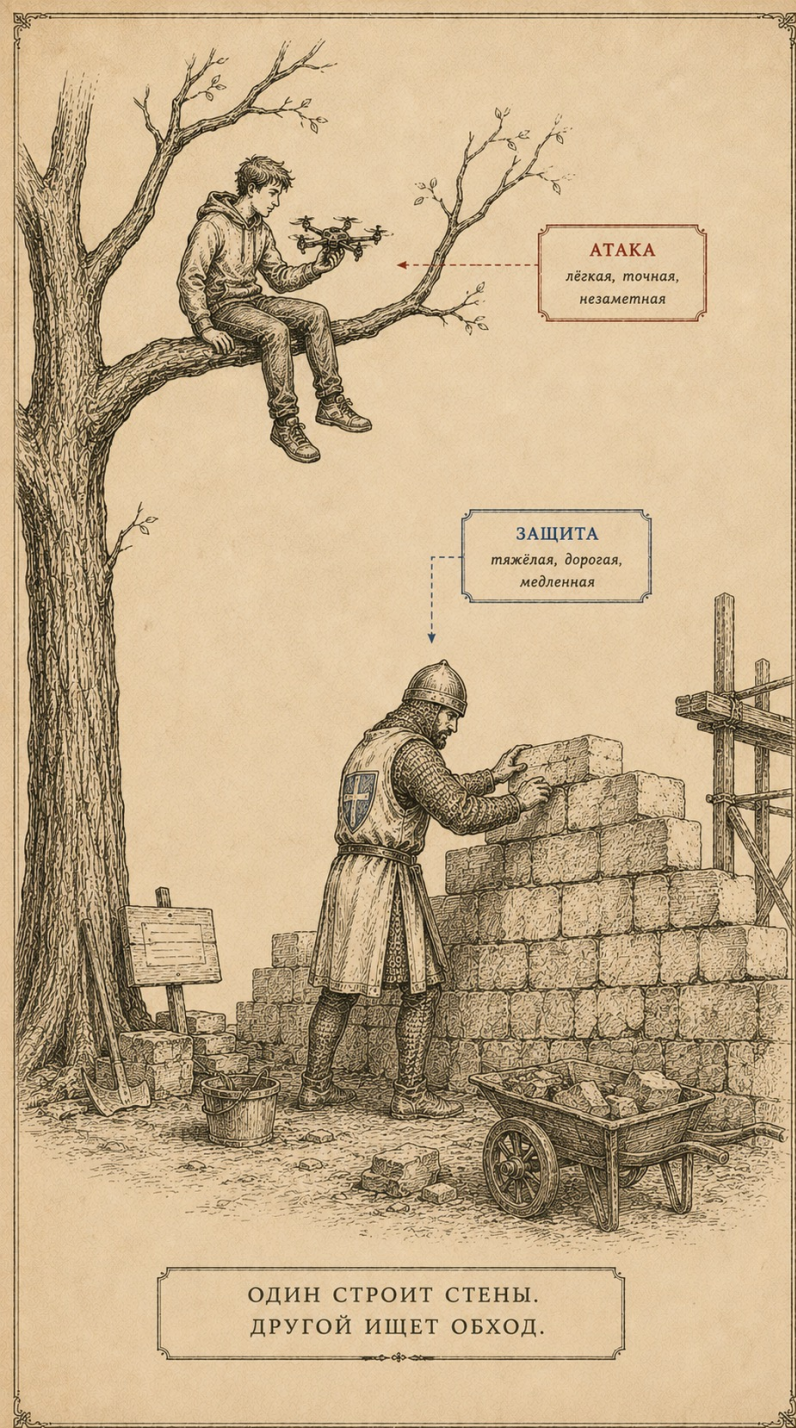
НЕ МОЩНОСТЬ.  
ЦЕНА.

СТРОИТЬ  
10 лет  
...  
очень дорого

СЛОМАТЬ  
за день  
...  
удивительно дешево

НОВОЕ ОРУЖИЕ  
МЕНЯЕТ НЕ СТЕНУ.  
ОНО МЕНЯЕТ ЕЁ ЦЕНУ.

удивительно дешево



# Когда страшно – человек строит стену

Когда атакующему становится дешевле разрушать, чем защитнику строить, стратегия защиты начинает проигрывать не в момент пробития стены, а еще на этапе бюджетирования

ДРОН ПРОТИВ КРЕПОСТИ

FPV-дрон  
≈ 500 \$Крепость  
строилась 10 лет  
стоимость защиты  
≈ 5 000 000 \$Толщина стены  
не знает цены.

№ 1759

# Дрон против крепости

Вспомните танки против дешевых дронов, корабли против морских беспилотников

НЕ РАЗМЕР РЕШАЕТ,  
А СКОРОСТЬ И ЧИСЛО

МАМОНТ

тяжёлый  
дорогой  
медленный  
заметный

РОЙ

лёгкий  
дешёвый  
быстрый  
вездесущий



СРАВНЕНИЕ



≈ 10 000 000 \$



≈ 500 \$

ИТОГ

МАМОНТ СИЛЕН.  
НО РОЙ РЕШАЕТ.

НОВАЯ ВОЙНА — ВОЙНА АСИММЕТРИИ.

# Противник **не** обязан быть равным

- Армия против армии
- Крепость против артиллерии
- Компания против хакерской группировки

# Нападающий

- Дешевле
- Быстрее
- Меньше
- Менее формальный
- Менее регулируемый
- Менее зависимый от согласований
- Менее озабоченный устойчивостью
- Готовый к потере ресурсов
- Способный повторять попытки почти бесплатно



# Защитник

- Дорогой
- Медленный
- Юридически ограниченный
- Зависимый от бизнеса
- Обязан не ломать систему
- Обязан объяснять бюджет
- Обязан соблюдать процессы
- Не может «просто попробовать»



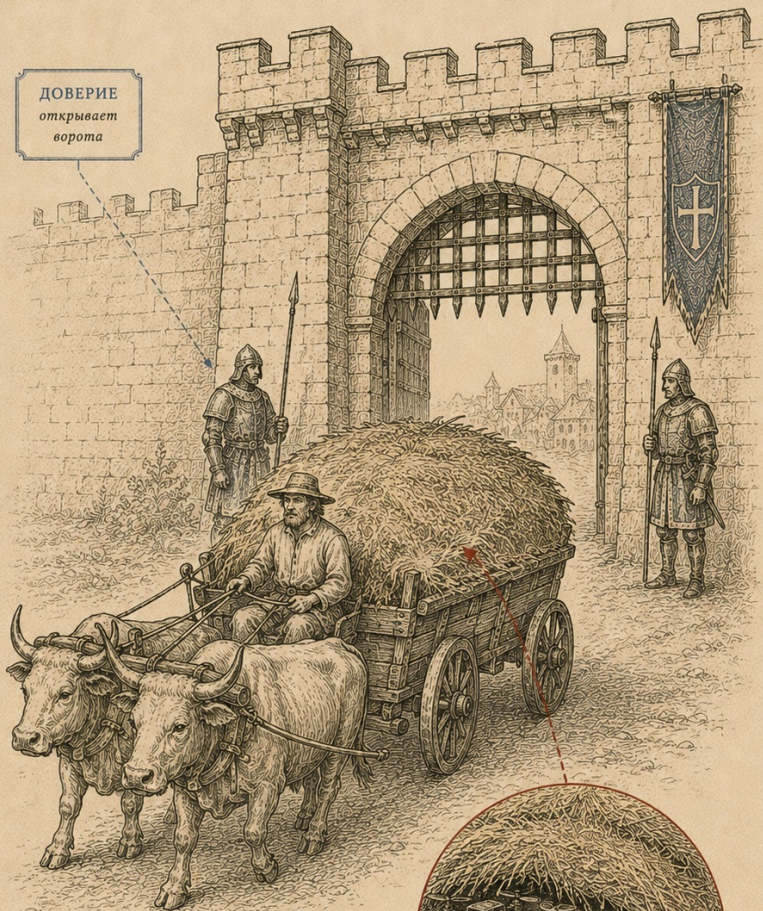
# Крепостное мышление

- ❑ Считать, что главное – не пустить
- ❑ Строить защиту вокруг границы, а не вокруг сценариев ущерба
- ❑ Добавлять контроль, не снижая цену защитного действия
- ❑ Мерить зрелость количеством стен
- ❑ Думать, что compliance = обороноспособность
- ❑ Верить, что «больше согласований» означает «больше безопасности»
- ❑ Защищать систему так, будто атакующий будет идти по официальному маршруту



АТАКА — НЕ ВСЕГДА ШТУРМ.  
ИНОГДА — ПОСТАВКА.

ДОВЕРИЕ  
открывает  
ворота



ПОДРЯДЧИК.  
ПОСТАВЩИК.  
ПАРТНЁР.  
доступ внутрь

ГРУЗ  
не вызывает  
подозрений

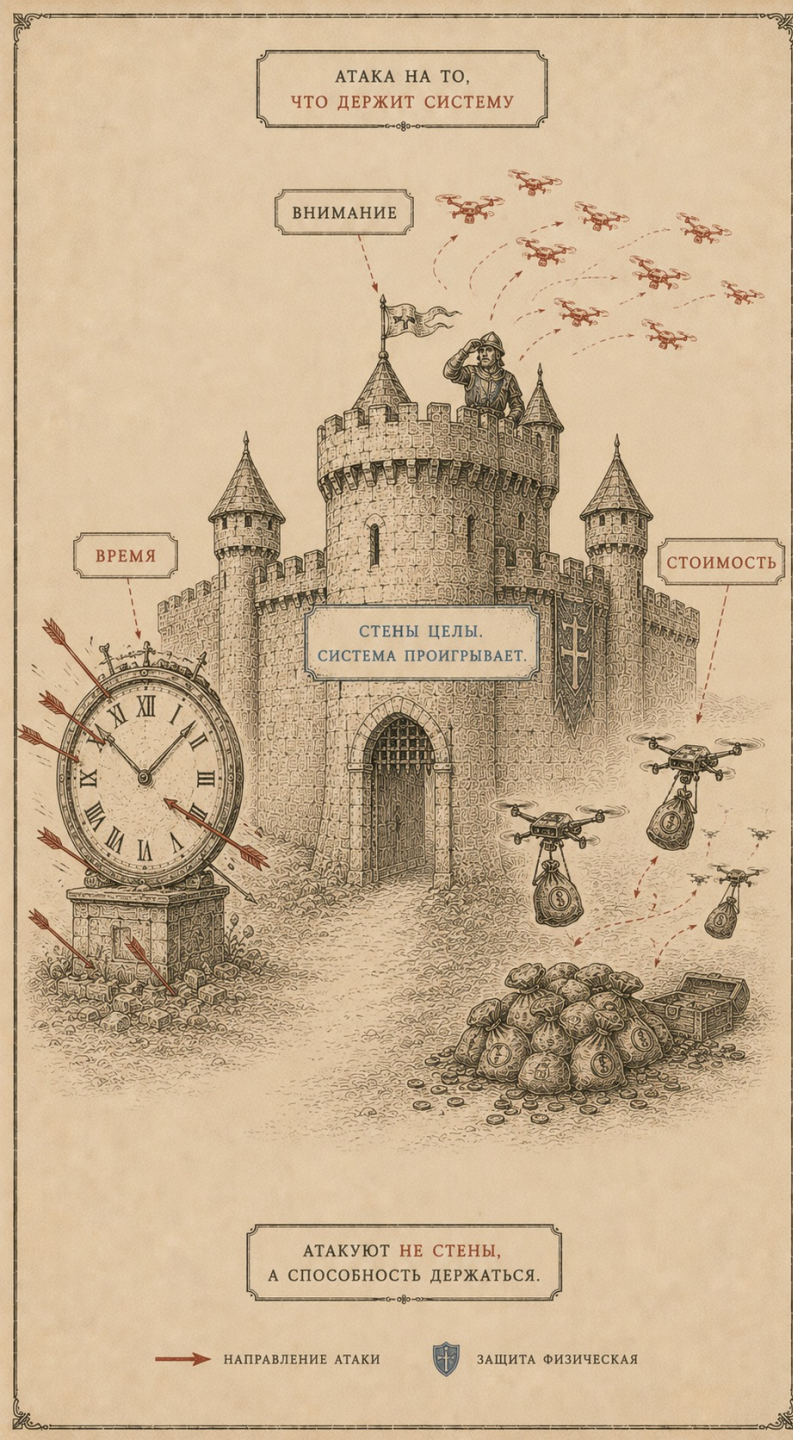
СОВРЕМЕННАЯ УГРОЗА  
не ломает стены.  
она входит с пропуском.

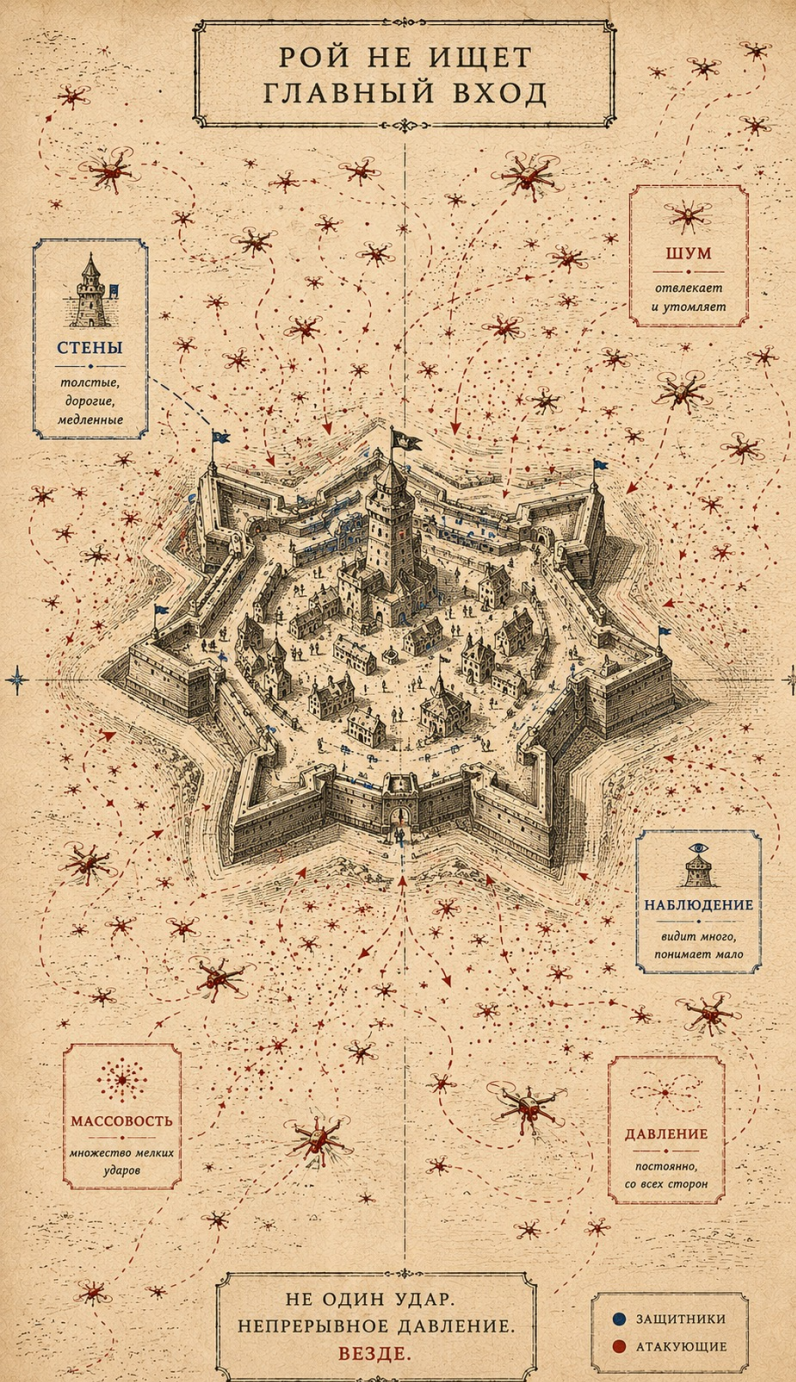
# Не обязательно атаковать стену

- Не ломает firewall, а крадет учетку
- Не пробивает SOC, а создает шум
- Не атакует crown jewels напрямую, а идет через подрядчика
- Не пишет уникальный 0-day, а массово ищет одинаковые ошибки
- Не «штурмует крепость», а меняет экономику ее обслуживания

# Атакуют не стену, а СТОИМОСТЬ, время. ВНИМАНИЕ

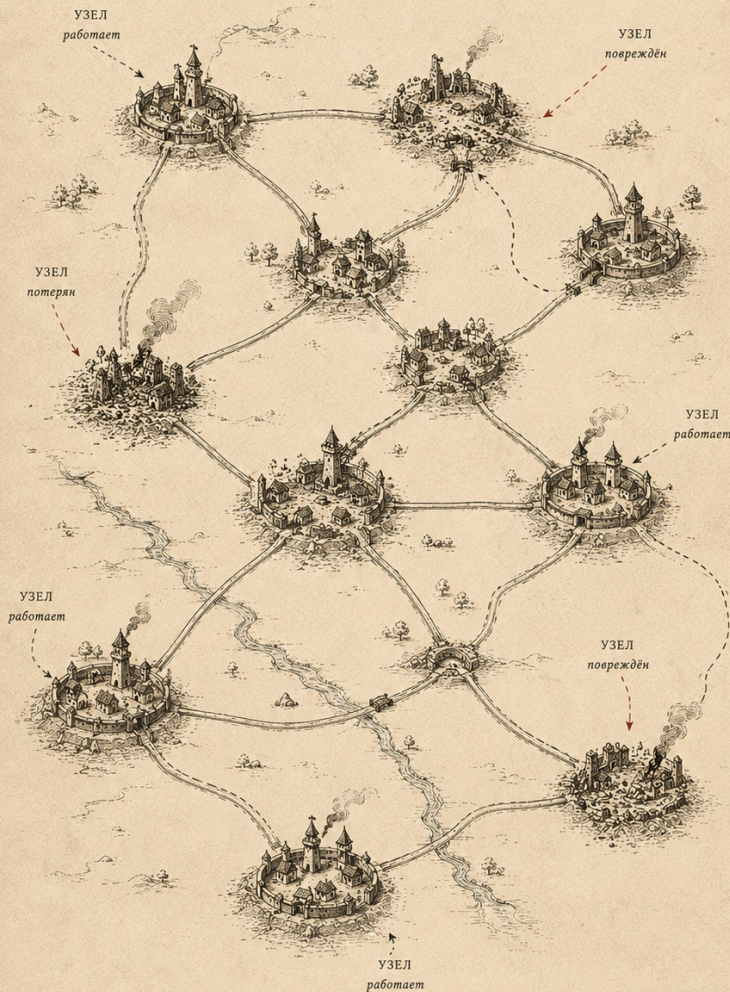
Современный атакующий не обязательно хочет победить вашу защиту. Ему достаточно сделать так, чтобы ваша защита стала слишком дорогой, слишком медленной или слишком бесполезной





# Никакого главного удара

НЕ НЕПРИСТУПНОСТЬ.  
ЖИВУЧЕСТЬ.



— ОСНОВНЫЕ СВЯЗИ  
- - - АЛЬТЕРНАТИВНЫЕ ПУТИ

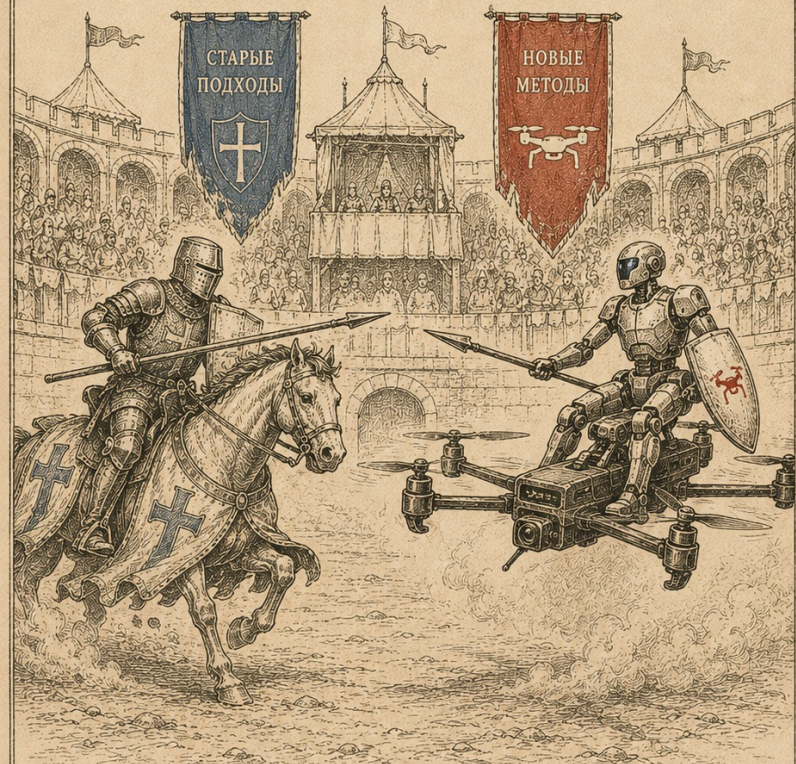
ЧАСТЬ ПОД УДАРОМ.  
СЕТЬ ПРОДОЛЖАЕТ ЖИТЬ.

ДЕЦЕНТРАЛИЗАЦИЯ — ЭТО УСТОЙЧИВОСТЬ.  
УСТОЙЧИВОСТЬ — ЭТО ПРЕИМУЩЕСТВО.

**Старая цель:**  
не пустить врага внутрь

**Новая цель:**  
сделать так, чтобы  
проникновение, сбой или  
компрометация не  
превращались в  
катастрофу

## ТУРНИР НОВОЙ ЭПОХИ



## РЫЦАРЬ

СИЛА  
ЧЕСТЬ  
ТЯЖЕЛАЯ БРОНЯ  
ДОЛГИЙ ПУТЬ  
ЯСНЫЕ ПРАВИЛА



## ДРОН-ВСАДНИК

СКОРОСТЬ  
ТОЧНОСТЬ  
ЛЁГКИЙ  
ДОСТУП ИЗ ЛЮБОЙ ТОЧКИ  
ПРАВИЛА МЕНЯЮТСЯ



ФОРМА МЕНЯЕТСЯ.  
СУТЬ ОСТАЁТСЯ.

# Что приходит после крепости?

- Не толщина стены, а малый радиус поражения
- Не абсолютная защита, а дешевое защитное действие
- Не контроль всего, а только важного
- Не вера в доверенную внутренность, а постоянная проверка
- Не защита объекта, а защита функции
- Не героическая оборона, а жизнь под давлением
- Не один большой план, а адаптация



# Дрон против крепости – это не про дрона и не про крепость

Это про момент, когда одна сторона уже живет в новой логике, а другая все еще докупает сертифицированные кирпичи для старой стены и нанимает строителей с аккредитацией из реестра

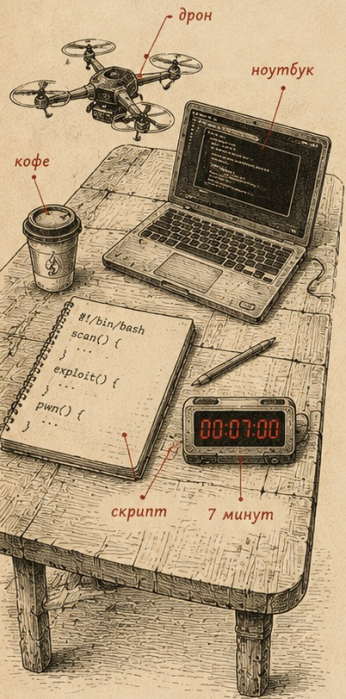
ОДНА ВОЙНА.  
РАЗНАЯ ЭКОНОМИКА.

**АТАКУЮЩИЙ**

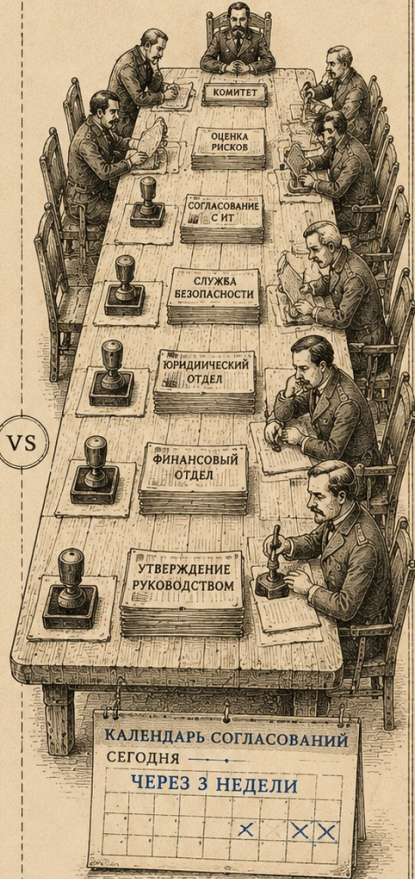
дешево, быстро,  
без согласований

**ЗАЩИТНИК**

дорого, медленно,  
много согласований



VS



**7 МИНУТ**

на поиск, решение  
и атаку

**ЧЕРЕЗ 3 НЕДЕЛИ**

если ничего  
не изменится

СКОРОСТЬ — ЭТО ТОЖЕ ОРУЖИЕ.  
ЭКОНОМИКА ВОЙНЫ РЕШАЕТ БОЛЬШЕ,  
ЧЕМ ТОЛЩИНА СТЕН.

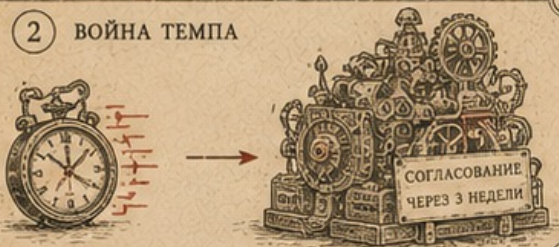
Самая опасная  
ошибка —  
проектировать  
безопасность для  
войны, которая уже  
закончилась

# Войны будущего: не сила, а асимметрия

1 ДЕШЁВОЕ ПРОТИВ ДОРОГОГО



2 ВОЙНА ТЕМПА



3 ВОЙНА РОЯ



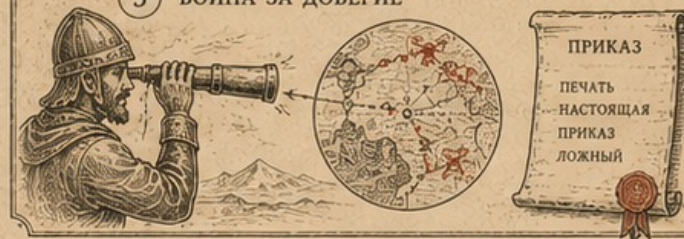
4 ВОЙНА СРЕД



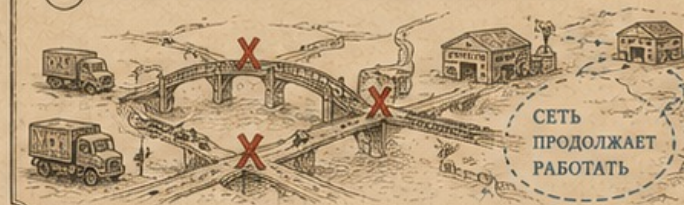
→ атака / давление  
 ← защита / устойчивость  
 ○ узлы и ресурсы



5 ВОЙНА ЗА ДОВЕРИЕ



6 ВОЙНА ЛОГИСТИКИ И ВОССТАНОВЛЕНИЯ



7 ЛЮДИ ПЛЮС МАШИНЫ



8 ВОЙНА АДАПТАЦИИ



Побеждает не неприступный, а тот, кто быстрее учится и продолжает действовать.

→ атака / давление    ← защита / устойчивость    ○ узлы и ресурсы

ПРИРОДА — ПЕРВЫЙ УЧИТЕЛЬ.  
НАБЛЮДЕНИЕ СОЗДАЁТ СТИЛИ.

МАСТЕР  
БОЕВЫХ ИСКУССТВ

ЛЕОНАРДО  
ДА ВИНЧИ

СОВРЕМЕННЫЙ  
ИНЖЕНЕР



КОБРА  
УДАР ИЗ ЗАСАДЫ

АИСТ  
ДИСТАНЦИЯ И КОНТРОЛЬ

БОГОМОЛ  
ГИБКОСТЬ И АДАПТАЦИЯ

СТРЕМИТЕЛЬНАЯ АТАКА  
СКРЫТНОСТЬ, ЯД

БАЛАНС, ДАЛЬНИЙ РЫЧАГ  
ТОЧНОСТЬ, ТЕРПЕНИЕ

ОЖИДАНИЕ, ПЕРЕХВАТ  
МАЛЕНЬКИЙ, НО ОПАСНЫЙ



СТИЛЬ АТАКИ

СТИЛЬ ЗАЩИТЫ

СТИЛЬ МАНЁВРА

РАЗНЫЕ ПОДХОДЫ. ОДНА ЦЕЛЬ — ПОБЕДА.  
НАБЛЮДАЙ. ПОНИМАЙ. ПРИМЕНЯЙ.

Крепости начинались с наблюдением за природой. Не пора ли вновь вернуться к наблюдениям?!

УЧИТЬСЯ СЕГОДНЯ —  
ПОБЕЖДАЙ ЗАВТРА



НОВЫЕ  
ЗНАНИЯ



НОВЫЕ  
СТРАТЕГИИ



НОВЫЕ  
ТЕХНОЛОГИИ



ПРЕВОСХОДСТВО  
В ЗАВТРАШНЕМ ДНЕ

СИЛА ПРОХОДИТ.  
ЗНАНИЕ ОСТАЁТСЯ.

# Дополнительные материалы

- Яковлев В.В. История крепостей
- Ткачев М.А. Замки Белоруссии
- Дмитрий Юрков. Советские «секретные бункеры»
- Цезарь Кюи. История крепостей Европы и России
- Лукацкий А.В. Информация под прикрытием: эволюция подходов к безопасности, от маскировки в дикой природе до средневековых замков и биохакинга
- Douglas J. Emlen. Animal Weapons: The Evolution of Battle
- Нассим Талеб. «Антихрупкость. Как извлечь выгоду из хаоса»

**Алексей Лукацкий**

Chief Evangelist Officer  
Positive Technologies



**Спасибо**

[alukatsky@ptsecurity.com](mailto:alukatsky@ptsecurity.com)



@ALUKATSK