ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

# Как заказать пентест и не остаться один на один со списком CVE

Александр Пушкин

Технический директор, «Перспективный мониторинг»

# Кто заказывал пентест?

## РЕАЛИЗОВАННЫЕ ПРОЕКТЫ


### Тестирование внешнего сетевого периметра «Финам»

АО «Инвестиционный холдинг ФИНА́М» (аббревиатура — «ФИНансовый Аналитик Москва») — крупнейший в России розничный брокер, а также инвестиционная группа, специализирующаяся на оказании трейдерских, инвестиционных банковских услуг, доверительном управлении денежными средствами и ценными бумагами, инвестировании на валютном рынке Forex.

Подробнее

Московская биржа

СПбМТСБ

Автоторгбанк

Финам

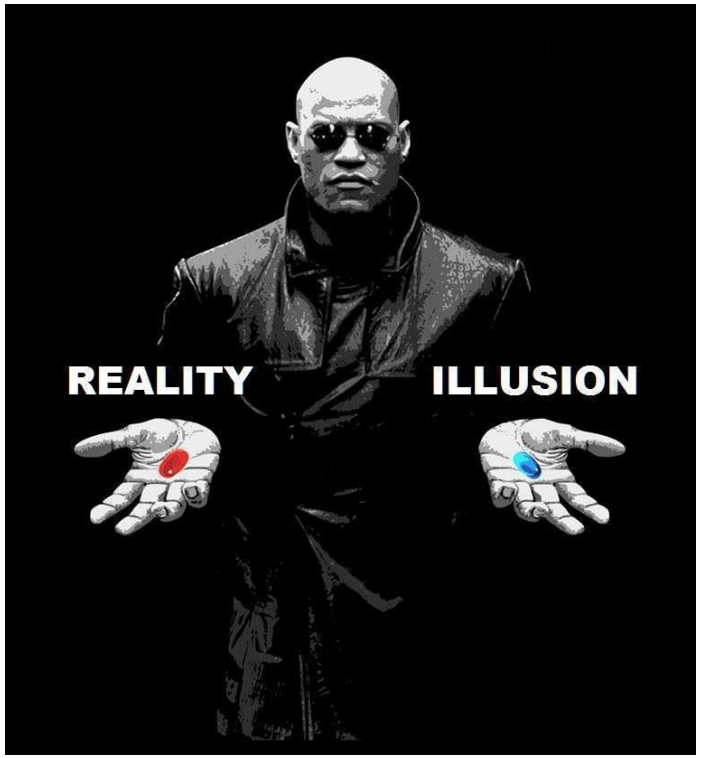
Эльдорадо

МТИ Банк

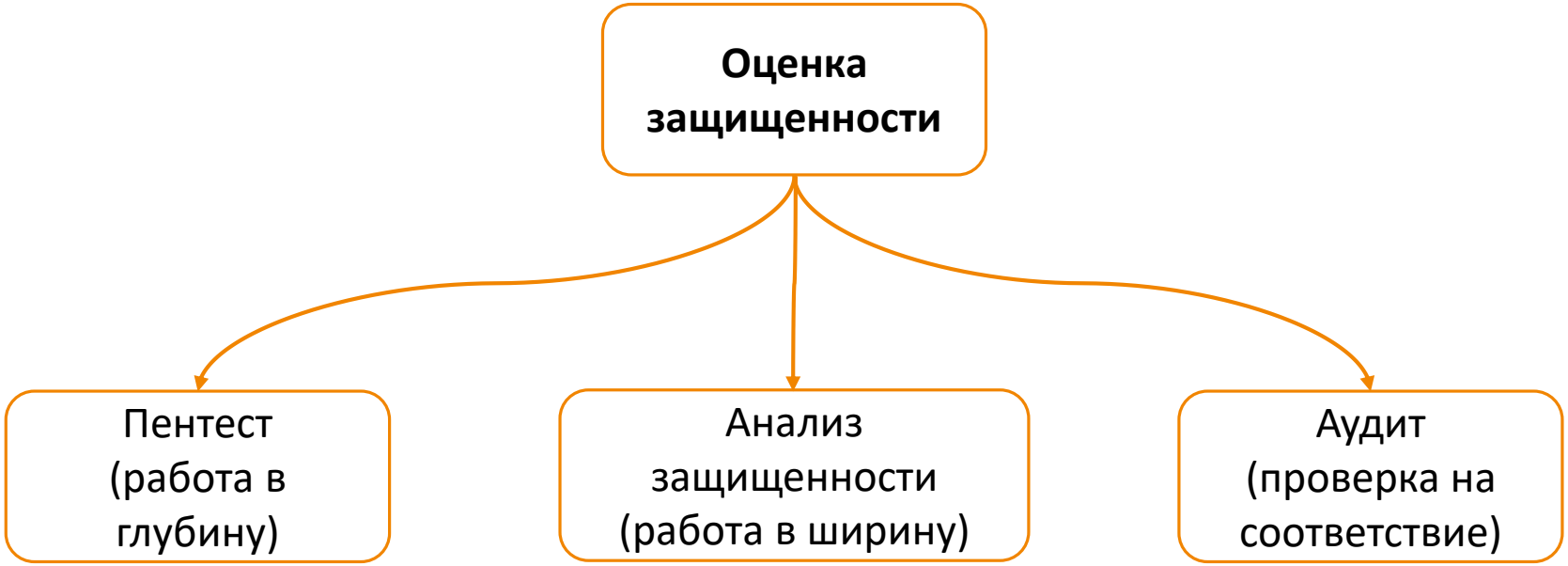
# С 2015 года 94 проекта по пентестам

# Что такое пентест?

**Пентест** – это комплекс технических мероприятий, который направлен на подтверждение/опровержение возможности успешного проведения компьютерной атаки (получение несанкционированного доступа, нарушение доступности и т.д.)



# Способы оценки защищенности ИБ



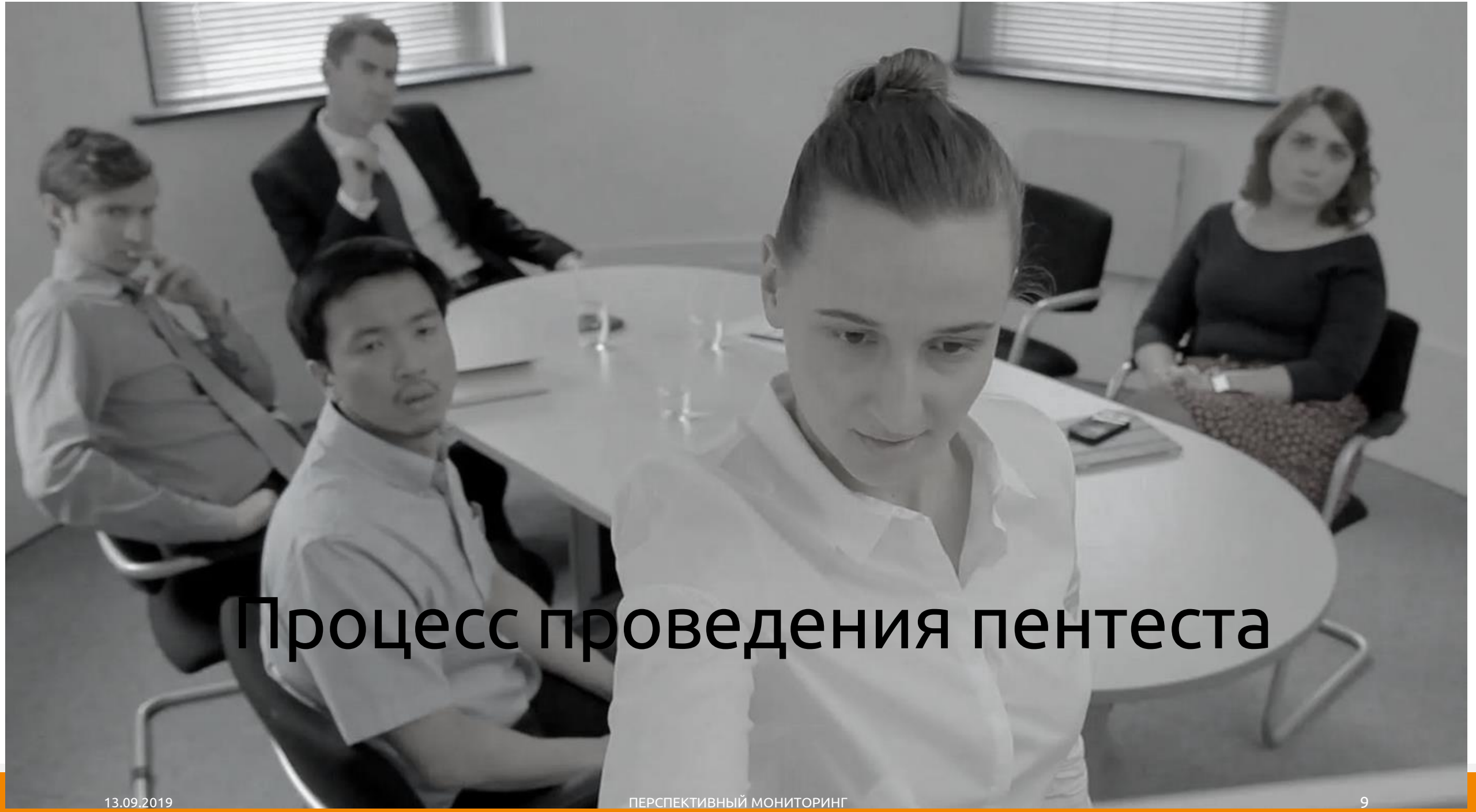
# Пентест – это тоже проект

# Требования к заказчику

1. Понимать для каких целей проводится пентест
2. Иметь в штате сотрудника соответствующей квалификации
3. Иметь ресурсы для исправления найденных уязвимостей/недостатков

# Требования к исполнителю

1. Опыт оценки защищенности аналогичных заказчику объектов
2. Длительное время существование на рынке
3. Портфель схожих проектов
4. Лицензии (ФСТЭК, техническая защита конфиденциальной информации)
5. Сертифицированные специалисты (OSCP, OSCE, CEH и т.д.)
6. Умение писать отчетные документы
7. Разработка действующих рекомендаций
8. Проведение исследовательских работ, участие в профильных конференциях



# Процесс проведения пентеста

# Анализ ТЗ

1. Какие объекты выделены для тестирования
2. Сроки
3. Модель нарушителя
4. Как осуществляется доступ к объектам

# Уточнение непонятных моментов

1. Что является критерием успешности пентеста
2. Кто из персонала уведомлен о проекте
3. Нужно ли сразу раскрывать критические уязвимости
4. С кем контактировать со стороны заказчика

| Цель | Критерии достижения |
|---|---|
| **Сайт** | Получение доступа к панели администрирования сайта и/или выполнениестороннего кода в контексте сайта. |
| **Корпоративная сеть** | Доступ к контроллеру домена корпоративной сети. |
| **Периметр корпоративной сети** | Выполнение стороннего кода на одном изхостов внешнего периметра. |

# Получение разрешения

**Приложение №4**
**к Договору № _____**
**от «__» _____ 201_ г.**

**РАЗРЕШЕНИЕ НА ПРОВЕДЕНИЕ РАБОТ**

**г. Москва** **«__» _____ 201_ г.**

Настоящее Разрешение на проведение работ по тестированию на проникновение подсистемы «Название» ИАС «Название», аудиту и контролю конфигурации серверной инфраструктуры, аудиту и контролю конфигурации АРМ, анализу защищенности внешнего периметра Компании, именуемое в дальнейшем **Разрешение**, выдается Компании в лице Должность Фамилия Имя Отчество, действующего на основании _____ (далее — «**Заказчик**»), Закрытому акционерному обществу «Перспективный мониторинг» (ЗАО «ПМ») в лице генерального директора Клименко Владимира Васильевича, действующего на основании Устава (далее — «**Соисполнитель**»), о нижеследующем:

1. Заказчик разрешает Соисполнителю и его сотрудникам, работающим в рамках выполнения обязательств по исполнению Государственного контракта № __ от «__» _____ 201_ г., заключенного между Компанией и _____, проводить действия, направленные на обнаружение и тестирование уязвимостей в информационных (ИС) и информационно-аналитических системах (ИАС) Заказчика, в том числе:
1.1. использовать ручной и полуавтоматический режим тестирования;
1.2. использовать автоматизированные и неавтоматизированные программно-аппаратные средства, реализующие сканирование и тестирование объектов информационных систем;
1.3. использовать передачу заведомо некорректных входных данных в целях выявления недекларированных возможностей и уязвимостей объектов исследования;
1.4. использовать имеющиеся к моменту начала проведения работ уязвимости в программном обеспечении и технических средствах;
1.5. использовать ошибки сетевой и серверной архитектуры.

2. Объектами исследования являются:
2.1. Подсистема «Название»;
2.2. Подсистема «Название»;
2.3. Подсистема «Название»;
2.4. Серверная инфраструктура;
2.5. АРМ;

1. Статья 272. Неправомерный доступ к компьютерной информации
2. Статья 273. Создание, использование и распространение вредоносных компьютерных программ

# Выполнение исследования

1. Автоматические инструменты/сканеры
2. Ручной способ
3. Стендирование
4. Реверс и дизассемблирование
5. Анализ исходных кодов
6. OSINT/социальная инженерия

# Подготовка отчета

1. Раздел для руководства
2. Раздел для технических сотрудников:
   a. Состав работ
   b. Выполненные исследования
   c. Описание найденных уязвимостей (что, на каком узле, как эксплуатировать, какие последствия, как исправлять)
   d. PoC найденных уязвимостей
   e. Рекомендации общего характера
3. Выводы

# Что делать с отчетом

1. Ознакомить всех ЗЛ
2. Применить (адаптировать и применить) рекомендации по устранению уязвимостей/недостатков
3. Провести анализ и попробовать выявить схожие проблемы в других ИС
4. Использовать отчет при следующих пентестах

# Алгоритм для эффективного проведения пентеста

1. Определить границы объекта исследования
2. Составить ТЗ (сроки, цели, время исследования, ответственные)
3. Сделать шортлист компаний-исполнителей
4. Встретиться с представителями компаний, «прощупать» компетенции
5. Провести конкурсные процедуры*
6. Заключить договор с победителем
7. Выдать разрешение на пентест
8. Контролировать каждый этап
9. Согласовать отчет
10. Использовать отчет в повышении уровня защищенности

Пентестер перед погружением в ИТ-инфраструктуру организации

VS

Пентестер, разобравшийся в инфраструктуре организации

# Спасибо за внимание!


## Александр Пушкин

Технический директор

компании «Перспективный мониторинг»

Aleksandr.Pushkin@amonitoring.ru